anand guru

SOC EXPERTS

Interview Questions on
Computer Networking

Anand Guru

Security+ | CySA+ | CEH | ECIH

Founder

SOC Experts

https://socexperts.com

Network Device

What is a Hub?

Hub is a layer 1 device that connects multiple computers. Hub is usually terms as ‘dumb’ device because it broadcasts all the data to every port.

What is a Switch?

Switch is a layer 2 device that connect two or more computers.

Switch can decide which computer is the message intended for and send the message directly to the right computer (instead of a broadcast).

What is a Router?

Router is a layer 3 device that connect 2 or more networks.

Routers can calculate the best route for sending data from one point to another using routing protocols.

What are the ranges of Private IP?

Private IP addresses are also called as **Non-Routable IP Addresses.**

The ranges are		CIDR format
Class A	10.0.0.0 – 10.255.255.255	10.0.0.0/8
Class B	172.16.0.0 – 172.31.255.255	172.16.0.0/12
Class C	192.168.0.0 – 192.168.255.255	192.168.0.0/16

What is NAT?

NAT Stands for **Network Address Translation**

It is the process of converting one IP to another. Usually a Private IP to a Public IP and vice versa.

What is PAT?

PAT stands for **Port Address Translation**

PAT permits multiple devices on a LAN to be mapped to a single public IP address. The goal of PAT is to conserve public IP addresses.

Example:

If traffic to 100.20.30.40 is coming on **Port 22** → NAT that to 10.10.5.6 (A Linux server)

If traffic to 100.20.30.40 is coming on **Port 443** → NAT that to 10.10.5.7 (Web server)

Commonly used Port Numbers

Protocol	Service	Port Number
FTP	File Transfer Protocol	20, 21
Telnet	Telnet	23
SSH	Secure Shell	22
SMTP	Simple Mail Transfer Protocol	25
DNS	Domain Name System	53
DHCP	Dynamic Host Configuration Protocol	67, 68
HTTP	Hyper Text Transfer Protocol	80
POP3	Post Office Protocol	110
NTP	Network Time Protocol	123
NetBIOS	NetBIOS Name Service	135 - 139
IMAP	Internet Message Access Protocol	143

Protocol	Service	Port Number
SNMP	Simple Network Management Protocol	161, 162
LDAP	Lightweight Directory Access Protocol	389
HTTPS	Secure Hyper Text Transfer Protocol	443
MS SQL	Microsoft SQL	1433
MySQL	mySQL Database	3306
RDP	Remote Desktop Protocol	3389
Syslog	Used to send logs to remote server	514
TLS Syslog	Secure Syslog	6514
SFTP	Secure File Transfer Protocol	22
Secure SMTP	Secure Simple Mail Transfer Protocol	587

Networking Basic Command Line Tools.

- How to find the IP address of a machine?
  `ipconfig`

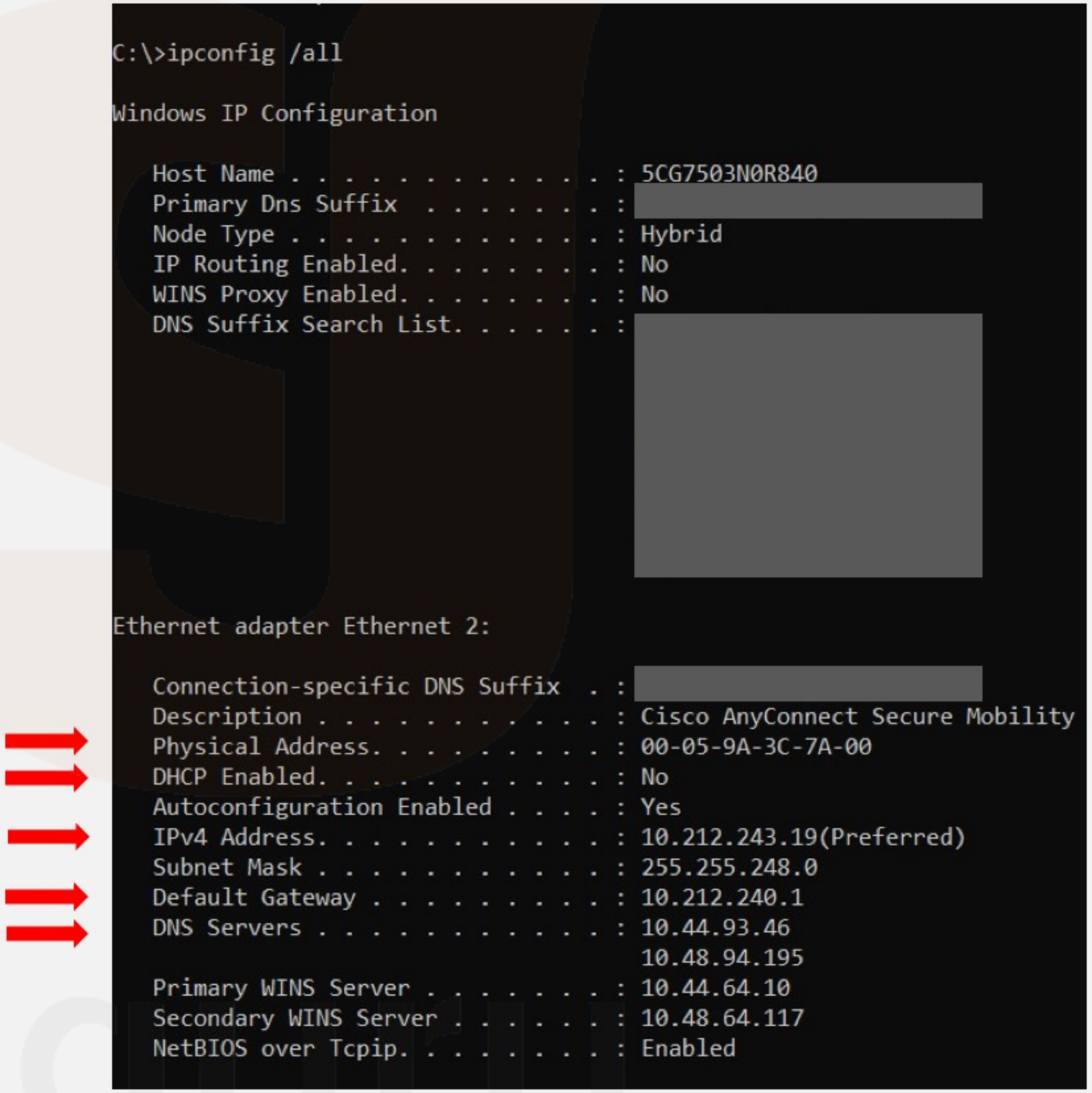
- How to find the MAC address of a machine?
  `ipconfig /all`

- What is MAC address listed as in Windows machine?
  Physical Address

- How do you find if DHCP is enabled on a system?
  `ipconfig /all`

- How do you find the Default Gateway on the system?
  `ipconfig /all`

- How do you find DNS servers on a system?
  `ipconfig /all`



```
C:\>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : 5CG7503N0R840
   Primary Dns Suffix  . . . . . . . : [redacted]
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : [redacted]

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : [redacted]
   Description . . . . . . . . . . . : Cisco AnyConnect Secure Mobility
   Physical Address. . . . . . . . . : 00-05-9A-3C-7A-00
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.212.243.19(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.248.0
   Default Gateway . . . . . . . . . : 10.212.240.1
   DNS Servers . . . . . . . . . . . : 10.44.93.46
                                       10.48.94.195
   Primary WINS Server . . . . . . . : 10.44.64.10
   Secondary WINS Server . . . . . . : 10.48.64.117
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Networking Basic Command Line Tools.

- How do you check if the destination machine is up and running or reachable?

  `ping`

- How to check if a port is open on the destination server?

  `telnet`

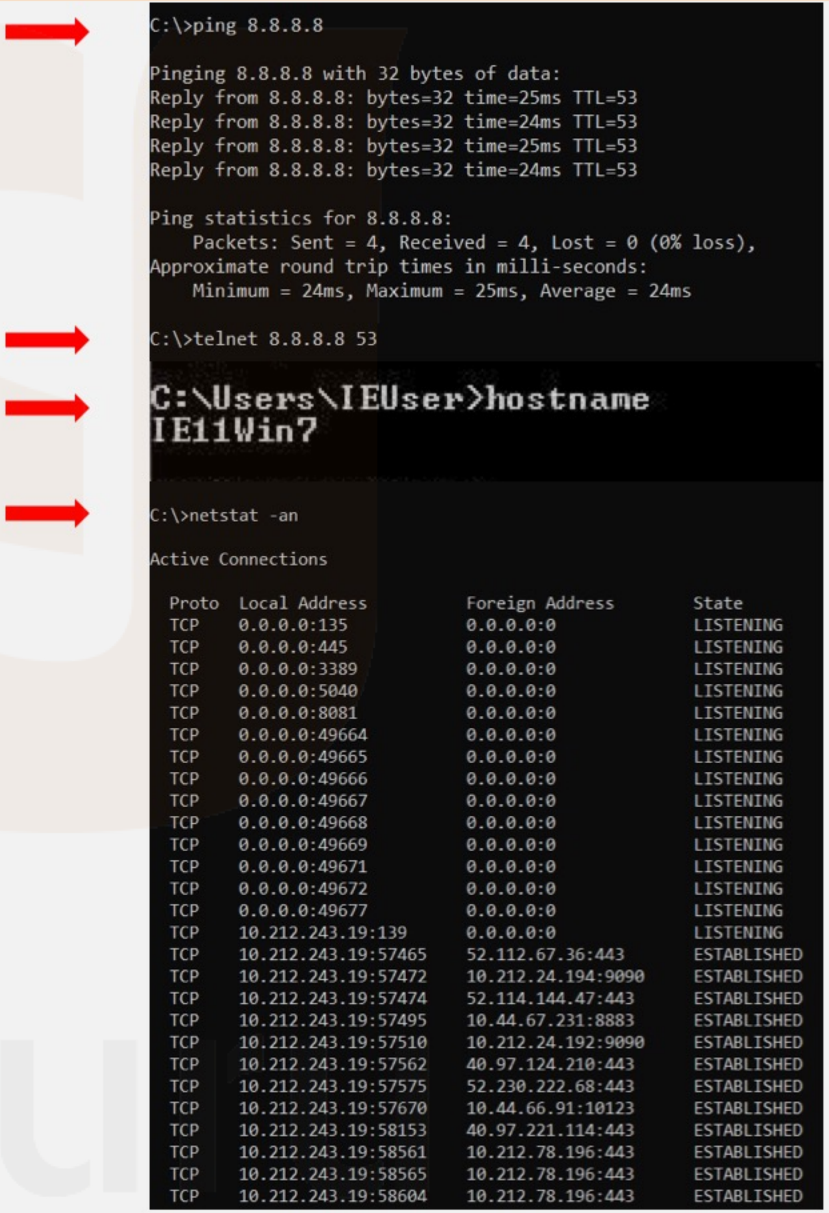
  telnet is done on the port in question.

- How to get the hostname of a machine?

  `hostname`

- How do you check open port on a machine?

  `netstat -an`



```
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=25ms TTL=53
Reply from 8.8.8.8: bytes=32 time=24ms TTL=53
Reply from 8.8.8.8: bytes=32 time=25ms TTL=53
Reply from 8.8.8.8: bytes=32 time=24ms TTL=53

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 24ms, Maximum = 25ms, Average = 24ms
```

```
C:\>telnet 8.8.8.8 53
```

```
C:\Users\IEUser>hostname
IE11Win7
```

```
C:\>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8081           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49672          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49677          0.0.0.0:0              LISTENING
  TCP    10.212.243.19:139      0.0.0.0:0              LISTENING
  TCP    10.212.243.19:57465    52.112.67.36:443       ESTABLISHED
  TCP    10.212.243.19:57472    10.212.24.194:9090     ESTABLISHED
  TCP    10.212.243.19:57474    52.114.144.47:443      ESTABLISHED
  TCP    10.212.243.19:57495    10.44.67.231:8883      ESTABLISHED
  TCP    10.212.243.19:57510    10.212.24.192:9090     ESTABLISHED
  TCP    10.212.243.19:57562    40.97.124.210:443      ESTABLISHED
  TCP    10.212.243.19:57575    52.230.222.68:443      ESTABLISHED
  TCP    10.212.243.19:57670    10.44.66.91:10123      ESTABLISHED
  TCP    10.212.243.19:58153    40.97.221.114:443      ESTABLISHED
  TCP    10.212.243.19:58561    10.212.78.196:443      ESTABLISHED
  TCP    10.212.243.19:58565    10.212.78.196:443      ESTABLISHED
  TCP    10.212.243.19:58604    10.212.78.196:443      ESTABLISHED
```

Explain the difference Between TCP and UDP.

	TCP	UDP
✓	Transmission Control Protocol	User Datagram Protocol
✓	Connection Oriented	Connection Less
✓	Acknowledgement for each packet transmitted	No Acknowledgement
✓	Failed packets are retransmitted	No re-transmission
✓	Guaranteed delivery	Best effort delivery
✓	Reliable	Unreliable
✓	TCP is slower	UDP is faster
✓	Example: HTTP, HTTPS, SMTP, SSH etc.	Streaming Videos, VOIP Calls, Online Games etc.

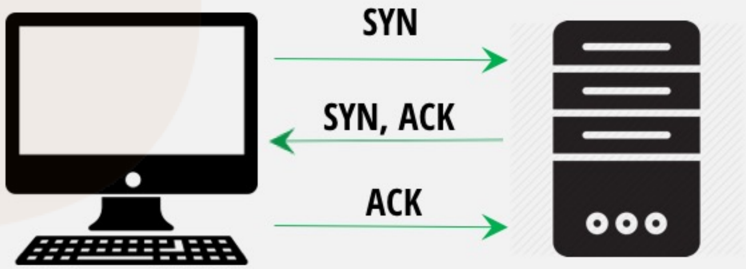
Explain 3 way handshake.

A three-way handshake is a method used in a TCP/IP network to create a connection between two hosts.

It is a 3 step process that requires both the client and server to exchange SYN and ACK (acknowledgment) packets before actual data communication begins.

Process is as Follows:

- A client node sends a **SYN** data packet to a server it wants to communicate to. The objective of this packet is to ask/infer if the server is open for new connections.
- If the server is willing to communicate to the client (if the port is open) it responds with an ACK packet.
  - It also expresses its intention of talking back to the client with its SYN packet.
  - Together it is **SYN/ACK**
- The client node responds with an **ACK** for the server's SYN.



Upon completion of this process, the connection is created and the host and server can communicate.

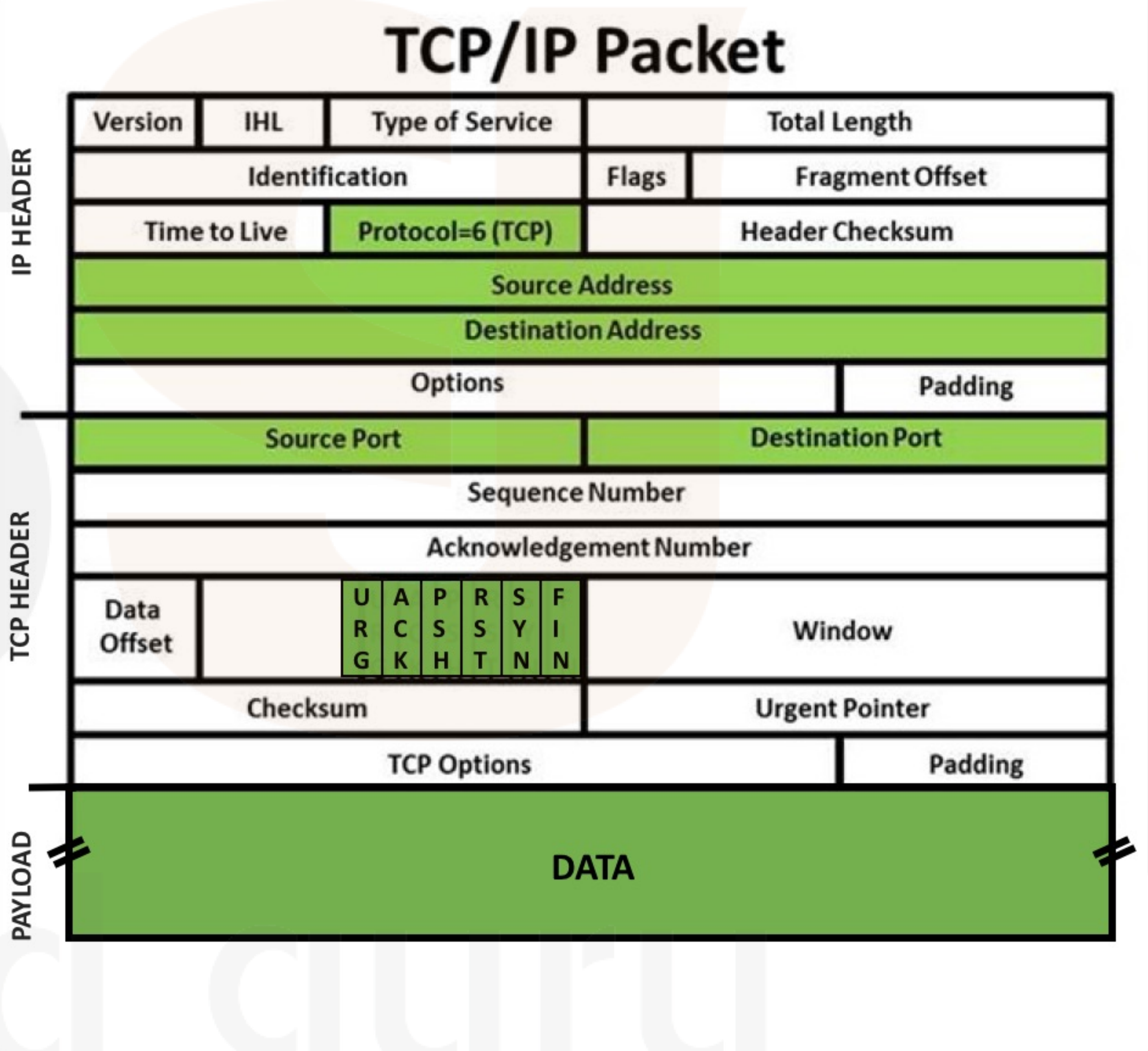
Explain Packet Structure.

A packet has 3 main sections

- IP Header
- TCP Header
- Payload

Few of the important fields in the packets are

- Source IP
- Destination IP
- Source Port
- Destination Port
- TCP Flags
- Data

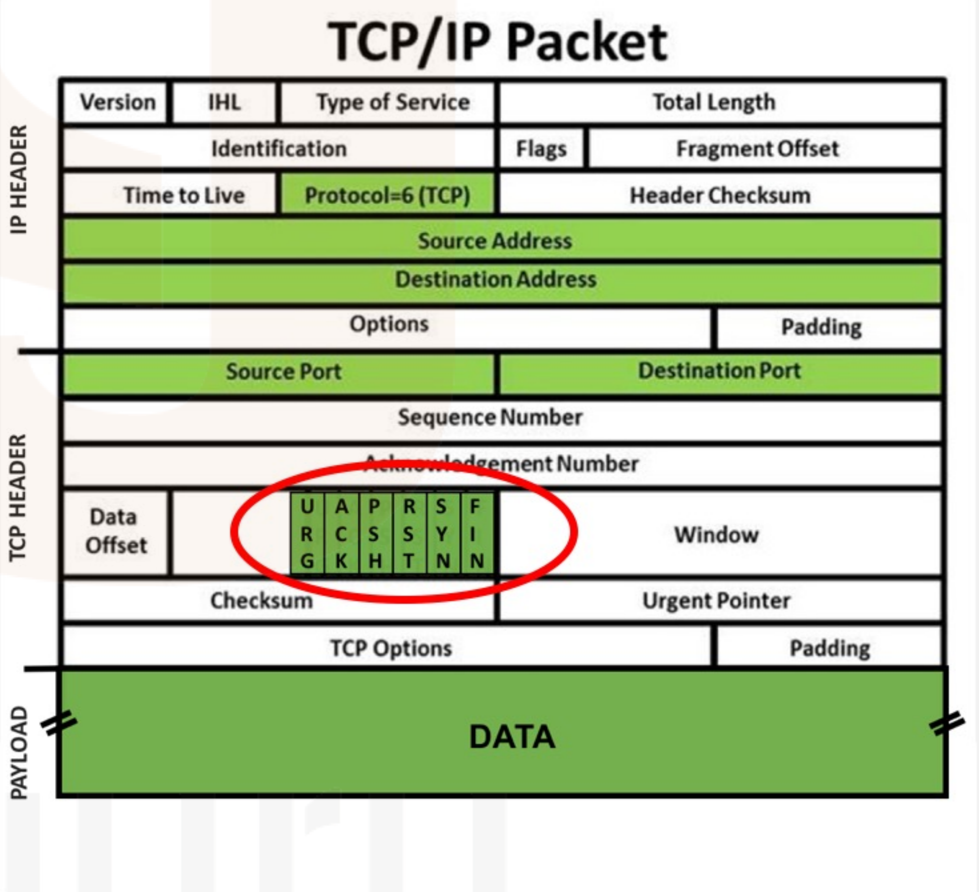


Explain TCP Flags.

In TCP connection, flags are used to indicate a particular state of connection.

There are 6 Flags in a TCP Header

Flag	Description
SYN (Synchronization)	It is used in first step of connection establishment phase or 3-way handshake process between the two hosts.
ACK (Acknowledgement)	It is used to acknowledge packets which are successful received by the host.
FIN (Finish)	It is used to request for connection termination i.e. when there is no more data from the sender, it requests for connection termination.
RST (Reset)	It is used to terminate the connection if the RST sender feels something is wrong with the TCP connection or that the conversation should not exist
PSH (Push)	It tells the receiver to process these packets as they are received instead of buffering them.
URG (Urgent)	Data inside a segment with URG = 1 flag is forwarded to application layer immediately even if there are more data to be given to application layer.



TCP/IP Packet

IP HEADER

Version | IHL | Type of Service | Total Length

Identification | Flags | Fragment Offset

Time to Live | Protocol=6 (TCP) | Header Checksum

Source Address

Destination Address

Options | Padding

TCP HEADER

Source Port | Destination Port

Sequence Number

Acknowledgement Number

Data Offset | URG | ACK | PSH | RST | SYN | FIN | Window

Checksum | Urgent Pointer

TCP Options | Padding

PAYLOAD

DATA

Explain OSI Reference Model.

Layer No.	Layer	Function	Devices	Protocols	PDU (Protocol Data Unit)
7	**APPLICATION**	• Interface between User and Computer. It provides services to the user. • Applications produce the data, which has to be transferred over the network.	-	HTTP, SMTP	Data
6	**PRESENTATION**	• The data from the application layer is extracted here and manipulated as per the required format to transmit over the network. • Translation (ASCII to HEX) • Encoding/Decoding • Encryption/Decryption • Compression	-	JPEG, MPEG, TLS, SSL	Data
5	**SESSION**	• This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.	-	NetBIOS, NFS, RPC	Data
4	**TRANSPORT**	• It provides reliable message delivery from process to process • Ensures that messages are transmitted in the order in which they are sent and there is no duplication of data. • It is also responsible for error control and flow control	-	TCP/UDP	Segments
3	**NETWORK**	• Network layer works for the transmission of data from one host to the other located in different networks. • Takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available.	Routers, Firewall, IPS	RIP, OSPF	Packets
2	**DATA LINK**	• The data link layer is responsible for the node to node delivery of the message. • It does Framing, error control, flow control etc. • Data Link Layer is divided into two sub layers : • Logical Link Control (LLC) • Media Access Control (MAC)	Switch	ARP	Frames
1	**PHYSICAL**	• It is responsible for the actual physical connection between the devices.	Hub, Bluetooth, WiFi	802.11	Bits

Explain OSI model with an example.

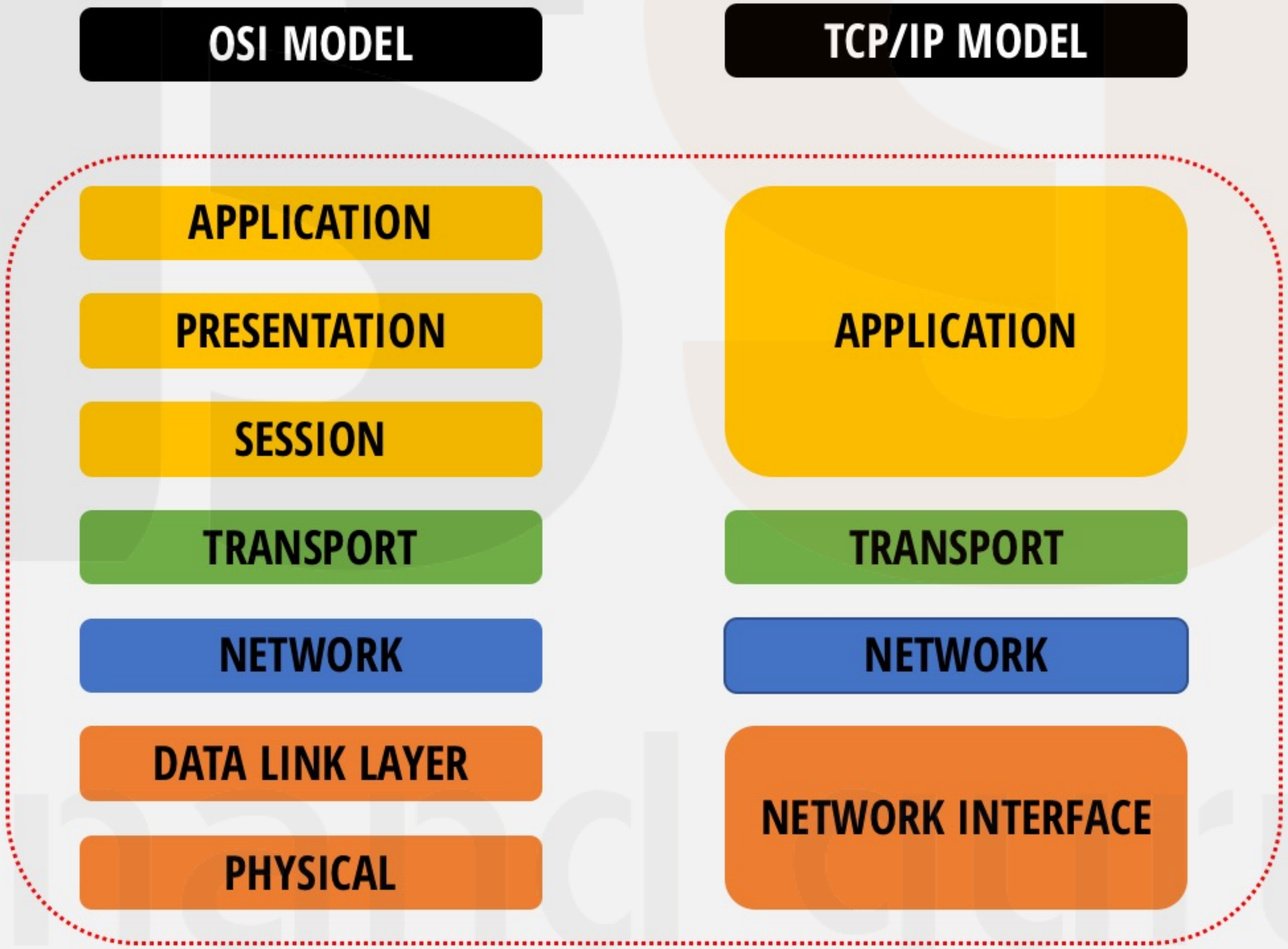
Lets discuss how email flows between sender and recipient using OSI model.

1. Sender uses an application like Outlook to compose and send the email. - **APPLICATION**
2. The email is encoded, encrypted (if enabled) and compressed. - **PRESENTATION**
3. The sending server initiates the connection with the receiving server. - **SESSION**
4. The entire email flows is done error free, receiving acknowledges. - **TRANSPORT**
5. Each packet will be routed from sender email server to recipient email server. - **NETWORK**
6. Node to Node transmission happens using next hop's MAC address. - **DATA LINK LAYER**
7. All the data is transmitted as bits through cables or wireless signals. - **PHYSICAL**

One the recipients side, the data moves from cable to users machine, where the presentation layer will take care of decoding, decrypting and decompressing the data. Finally the Outlook application will display the message to the recipient

Explain TCP/IP Model

OSI is a reference model, where as TCP/IP model is a practical model. The functions remain the same, but few of the layers gets merged in TCP/IP model.



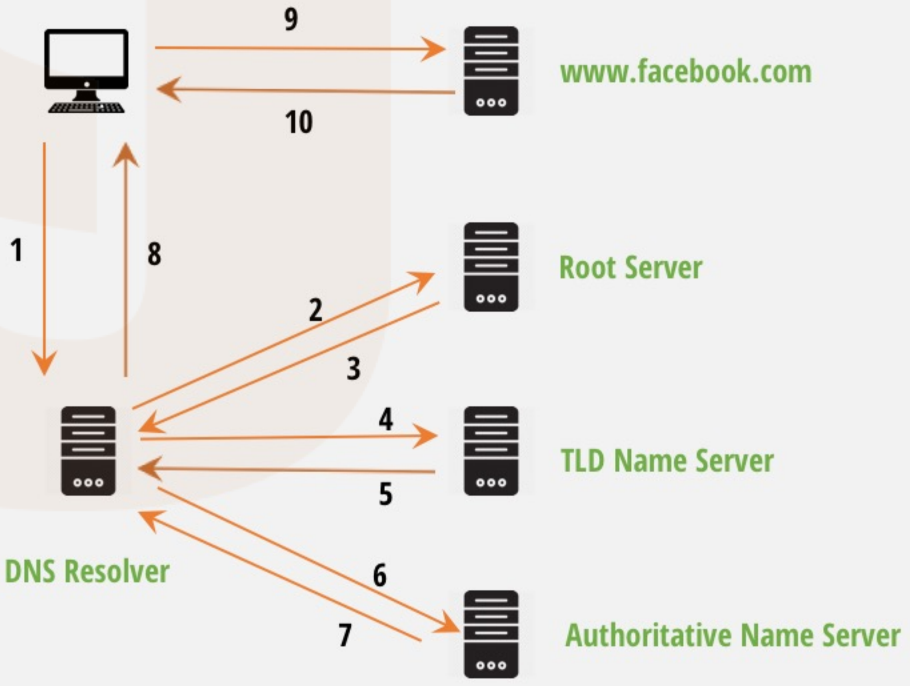
What is DNS and how it works?

DNS stands for Domain Name System.

It is a service that helps in translating domain names to IP addresses and vice versa.

How DNS works?

- When a computer needs to reach to a domain (like facebook.com) it sends a request to a server called **DNS Resolver** (DNS server). If the mapping is found for the domain in the DNS cache, the server returns the IP address. If not,
- The Resolver reaches out to **Root Server**. Root Servers hold the index of a Top Level Domains. There are 13 root servers globally.
- **TLD Name Server** gives the IP address of the Authoritative Name Server that holds the mapping for the requested domain name.
- If the **Authoritative Name Server** has access to the requested record, it will return the IP address
- This address is return to the client that made the original request.
- The client now makes the request to the IP address and get the response



DNS follow-up questions.

Does DNS use UDP or TCP?

DNS uses both TCP and UDP

UDP for DNS Queries

TCP for Zone Transfers

DNS Records Types.

A	(Host address)
AAAA	(IPv6 host address)
ALIAS	(Auto resolved alias)
CNAME	(Canonical name for an alias)
MX	(Mail eXchange)
NS	(Name Server)
PTR	(Pointer)
SOA	(Start Of Authority)
SRV	(location of service)
TXT	(Descriptive text)

What is DHCP and how it works?

DHCP stands for Dynamic Host Configuration Protocol.

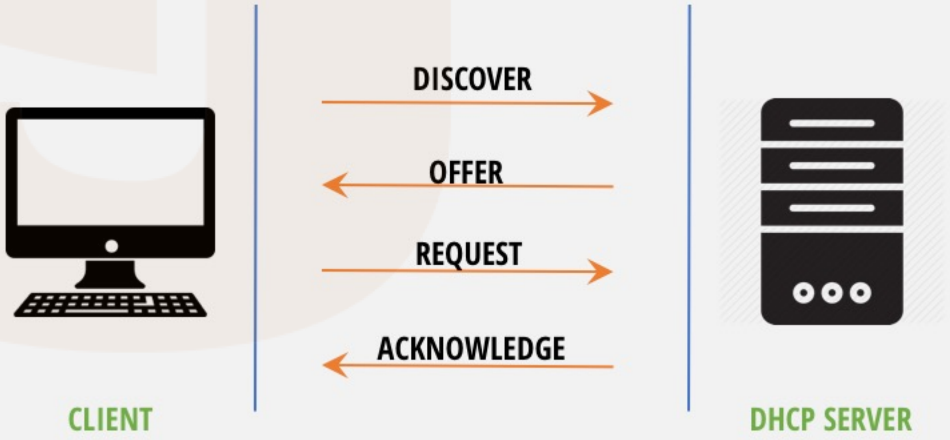
DHCP server automatically assigns an IP address and other information to each host on the network so they can communicate with other endpoints.

How DHCP works?

DHCP works on a process called DORA.

- When a computer that is configured to get the IP details automatically is powered on, it sends DHCP **DISCOVER** message to all hosts.
- After the DHCP Server receives discover message it suggests the IP addressing offering to the client host by unicast.

  This **OFFER** message contains: IP Address, Subnet mask, Default Gateway, DNS and Lease period
- Now after the client receives the offer it requests the information officially sending **REQUEST** message to server this time by unicast.
- Server sends **ACKNOWLEDGE** message confirming the DHCP lease to client. Now client is allowed to use new IP settings.



DHCP follow-up questions.

What will the IP address of the client machine when it sends DISCOVER message?

The Source IP will be 0.0.0.0

How does client knows the IP address of the DHCP Server, to send a Discover message?

The client would not be knowing the DHCP address, hence it broadcasts the Discover message. i.e. Destination IP will be 255.255.255.255

What happens if no DHCP server is available on the network?

The client gets an IP is the APIPA (Automatic Private IP Addressing) range. The range is between 169.254.0.0 - 169.254.255.255

What happens when the DHCP server runs out of IP addresses?

When you start running out of addresses, your subnet is said to be oversubscribed. Then the DHCP server refuse to assign an IP address until a device in the network releases an IP address and makes it available again or the lease time expires.

Explain ARP.

ARP stands for Address Resolution Protocol.

It helps to resolve an IP address to physical address (MAC Address)

How ARP works?

1. When a source device want to communicate with another device, source device checks its Address Resolution Protocol (ARP) cache to find it already has a resolved MAC Address of the destination device. If it is there, it will use that MAC Address for communication. If not, the source broadcasts the Address Resolution Protocol (ARP) request message to the local network.
2. The message is received by each device on the LAN since it is a broadcast. When the destination device receives the ARP request, it will send the Address Resolution Protocol (ARP) reply message to the source as a unicast.
3. The source machine will update its Address Resolution Protocol (ARP) cache.

What are proxy servers and how do they protect computer networks?

Proxy servers processes the request on behalf of other machines. The IP address is converted by NAT process.

Proxy servers primarily prevent external users from identifying the IP addresses of an internal network.

Without knowledge of the correct IP address, even the physical location of the network cannot be identified.

Proxy servers can make a network virtually invisible to external users.

When you use a proxy, is DNS query done by client or Proxy server?

It depends on the type of proxy being used.

If it is a simple **IP proxy**, then the client will do a DNS query, resolve the destination domain name and send the request to proxy.

If the proxy is a **HTTP proxy (Web Proxy),** the client directly send the request to proxy. Proxy requests for DNS resolution and forward the traffic.

Few random questions

Can you connect 2 computer directly?

Yes, with the help of cross-over cables.

I give you a new laptop, explain how you will connect to internet.

- Assuming the OS is already installed. I will look to assign the IP details like
  - IP Address
  - Subnet Mask
  - Default Gateway
  - DNS Server
- I will get these details from the network engineer who has designed the network.
- Alternately, if I there is a DHCP server in the network, I will configure the new laptop to automatically get the IP details.
- Then I ping any public IP like 8.8.8.8 to confirm if the laptop is able to reach the internet
- Also, ping any URL like www.google.com to check if DNS is working fine.

ICMP works on which layer?

ICMP works on Layer 3.

What port does ping use?

Ping uses ICMP(Internet Control Message Protocol). it does not use TCP or UDP. To be more precise ICMP type 8 (echo request message) and type 0 (echo reply message) are used. ICMP has no ports.

What happens when you type-in an URL (like www.goolgle.com) in your browser and press enter?

When you type in www.google.com into the address bar of browser,

1. The client needs to finds the IP address of the URL (in this case google.com).
    1. Browser check for if its cache to see if it has the IP address for entered domain
    2. If there is no IP mapping, it will check in OS cache.
    3. If the OS cache also doesn't have the IP address, the client initiates a DNS request to the configured DNS server.
2. Once the client has the IP address of the URL, the browser initiates a TCP connection with the server.
3. The browser sends an HTTP request to the webserver.
4. The server handles the request and sends back a response.
5. The browser displays the HTML content

Firewall related questions.

What is Firewall?

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules (ACL – Access Control List). Traditional firewalls works at Layer 3 and Layer 4.

When we can write ACLs in Router, why we need a Firewall?

Primary function of a router is to route the traffic. If we add packet filtering functions on to the router, it will slow down the network.

Hence it is a good practice to separate filtering and routing functionality

What is DMZ?

DMZ stands for DeMilitarized Zone. It is a network segment used to host public facing servers. The DMZ isolates the public facing servers from internal servers. So if the servers in DMZ are compromised, the attack doesn't spread to internal network.

What is Implicit Deny?

If traffic is not explicitly allowed within an access list then by default it is denied

What is the difference between Firewall Deny and Drop?

When the firewall is set to Deny a connection, it blocks the connection and sends a Reset (RST) packet to the requester (source).

When the firewall is set to Drop a connection, it just drops the requests without giving any message to the requester.

It is good practice to Deny outbound traffic and Drop inbound traffic, so the attacker will not know the presence of the Firewall.

What is Stateful Inspection?

A stateful firewall maintains a table of active connections it has allowed in a State Table. Further packets associated with the session are permitted to pass through the firewall.

What is VPN?

A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across public networks as if they were directly connected to the private network.

There are 2 types of VPN: **Site-to-Site VPN** – Used to connect two office locations. **Remote VPN** – Used by users to connect to corporate network

IPS/IDS related questions.

What is IDS?

An Intrusion Detection System is a network security solution that detects the malicious traffic based on the signatures. IDS systems compare the current network activity to a known threat database (network signatures) to detect several kinds of behaviors like security policy violations, malware, and port scanners.

Difference between IPS and IDS.

IDS scans the traffic and detects malicious traffic and report it to the admin based on network signature.

IPS scans the traffic, detects and can also block (prevent) the malicious traffic based on network signatures.

Explain IDS Signature syntax.

```
alert icmp any any -> $HOME_NET any (msg:”ICMP test”; sid:1000001; rev:1; classtype:icmp-event;)
```

Rule Header

`alert` – Rule action. Snort will generate an alert when the set condition is met.

`any` – Source IP. Snort will look at all sources.

`any` – Source port. Snort will look at all ports.

`->` – Direction. From source to destination.

`$HOME_NET` – Destination IP. We are using the HOME_NET value from the snort.conf file.

`any` – Destination port. Snort will look at all ports on the protected network.

Rule Options

`msg:”ICMP test”` – Snort will include this message with the alert.

`sid:1000001` – Snort rule ID.

`rev:1` – Revision number. This option allows for easier rule maintenance.

`classtype:icmp-event` – Categorizes the rule as an “icmp-event”, one of the predefined Snort categories.

Difference between IPS and Firewall.

A firewall inspects TCP/IP header working on ACLs.

IPS does deep packet inspection (checks both header and payload) using network signatures

Where do you place IPS?

An IPS is usually placed after the Firewall. Firewall does the heavy lifting of blocking all the unwanted traffic based on TCP/IP header. And of the traffic that is allowed, IPS will do deep packet inspection. Because of this IPS needs more processing power than a firewall.

If IPS is placed first, it will unnecessarily do deep packet inspection on all the traffic, while a good amount of traffic could have been blocked just by inspecting TCP/IP header with a packet filtering device like Firewall.

Questions on Linux commands

Sl. No.	Question	Command
1	Change Directory	**cd**
2	How do you check running process?	**ps auxf**
3	Disk statistics.	**df -h**
4	How do you find a file on Linux?	**find / <name_of_file>**
5	How do you kill a process in Linux?	**kill -9 <process_id>**
6	How do you get help on a command?	**man top** **top --help**
7	Create a new directory	**mkdir <new_directory_name>**
8	Change password	**passwd**
9	Present working directory	**pwd**
10	How do you open a text file to see the latest (last lines) during troubleshooting?	**tail –f <file_name>**
11	How do you display data regarding RAM and CPU?	**top**
12	Packet capture	**tcpdump –vvnni eth0**
13	How do you find the IP address on a Linux machine?	**ifconfig**

anand guru

SOC EXPERTS

Interview Questions on **Security Concepts**

Anand Guru

Security+ | CySA+ | CEH | ECIH

Founder

SOC Experts

https://socexperts.com

What is CIA?

Confidentiality, **Integrity** and **Availability**, also known as the **CIA triad**, is a model designed to guide policies for information security within an organization. The elements of the triad are considered the three most crucial components of security.

Component	Definition	How do you ensure?
Confidentiality	Confidentiality means that only the authorized individuals/systems can view sensitive or classified information. The data being sent over the network should not be accessed by unauthorized individuals.	Encryption Access Control
Integrity	Ensuring the data is not modified either in transit or at storage.	Hashing
Availability	Ensuring the systems and data is readily available to its users.	Redundancy Backups Load Balancers

What is Encryption? Explain types of encryption.

Encryption is the process of encoding information in such a way that only authorized parties can understand it.

Encryption is done using Keys.

There are 2 types of Encryption:

- **Symmetric Encryption** - Same key is used for encryption and decryption.
  - E.g.: Blowfish, AES, RC4, DES, RC5, and RC6
- **Asymmetric Encryption** - Different keys are used encryption and decryption.
  - E.g.: RSA, DSA, Elliptic curve techniques, PKCS.

Explain Asymmetric Encryption.

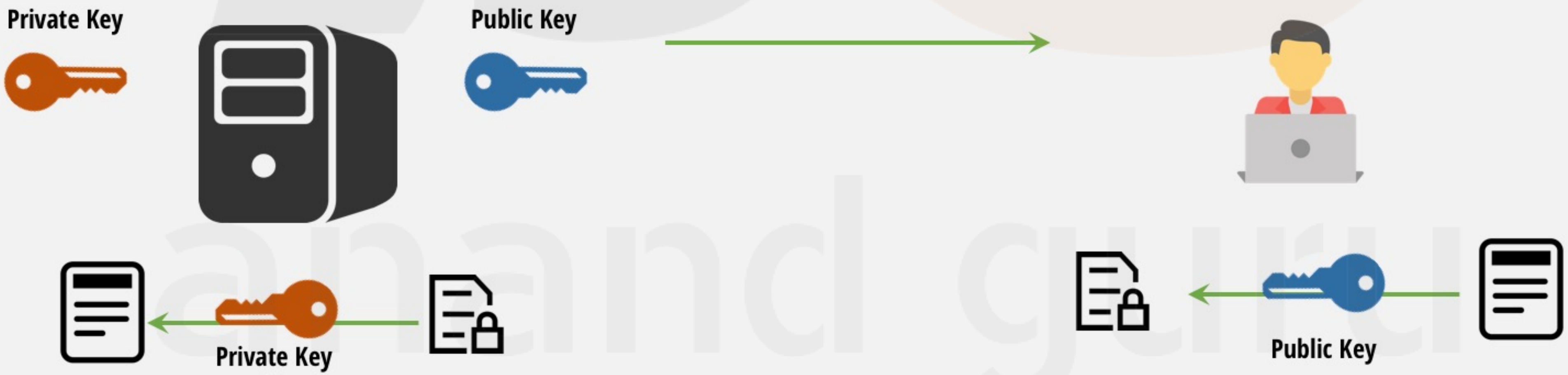
In asymmetric encryption different keys are used encryption and decryption.

Typically know as Private Key and Public Key (also referred to as Key Pair).

Any data encrypted with public key can only be decrypted by the corresponding private key.

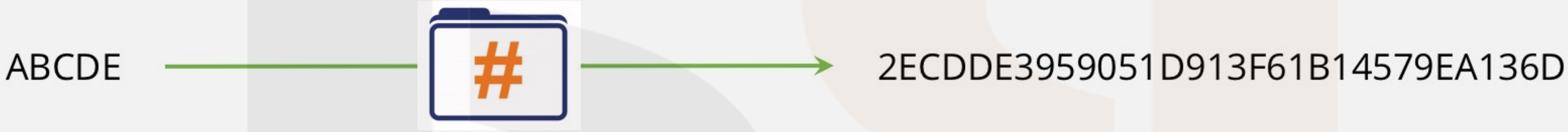
Example:

- A server keeps a key-pair. The public key is issued to all the users who request a connection.
- At the user’s end, the application encrypts the data using the server provided public key.
- Once the encrypted message reach the server, the server decrypts the message using its private key.



What is Hashing?

- Hashing is the transformation of a string of characters into a fixed-length value or key that represents the original string.



- Hashing is one-way. i.e. it is not possible to get the data back from the hash value.
- Hashing is used to ensure the integrity of the data.

E.g.:

• MD5	- 32 Hexadecimal characters
• SHA-1	- 40 Hexadecimal characters
• SHA-256	- 64 Hexadecimal characters

Explain difference between Encryption and Hashing.

Encryption	Hashing
Encryption is the process of encoding information in such a way that only authorized parties can understand it.	Hashing is the transformation of a string of characters into a fixed-length value or key that represents the original string.
Two-way. i.e. we can get the data back by decryption	One-way. i.e. we cannot get the data back from hash value
Used to ensure confidentiality	Used to ensure integrity
Algorithms: AES, DES, Bluefish	Algorithms: MD5, SHA-1, SHA-256

What is Vulnerability, Risk, Threat and Exploit?

Vulnerability Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset.

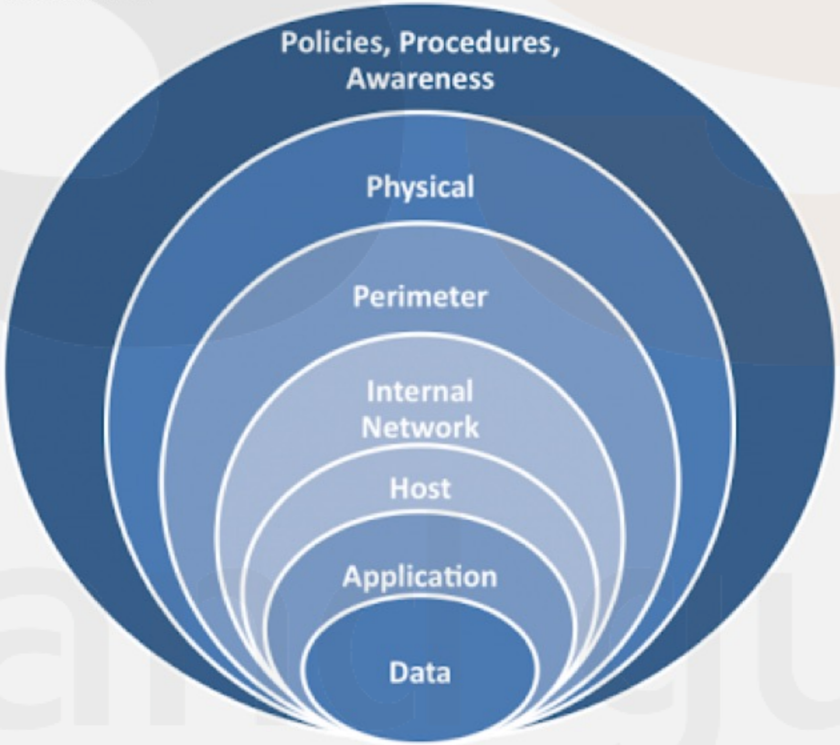
Risk The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability.

Threat Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.

Exploit The tool or mechanism used to take advantage of the vulnerability

Explain Defense in Depth.

- Defense in Depth (DiD) is an approach to cybersecurity in which a series of defensive mechanisms are layered in order to protect valuable data and information.
- If one mechanism fails, another steps up immediately to thwart an attack.
- This multi-layered approach with intentional redundancies increases the security of a system as a whole and addresses many different attack vectors.



What is System Hardening?

Systems hardening is a process of securing a system by reducing its attack surface.

Few things on the system hardening checklist include:

- Changing the default user credentials
- Closing all unused ports
- Stopping all unused services
- Install updates and patches
- Implement Access Control
- Install Antivirus and keep the signatures up-to-date

What is Zero Trust Model.

Zero trust security is an IT security model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter.

Few principles of zero trust model are:

- Assume there are attackers both inside and outside the network
- Concept of least privilege
- Use Multi Factor Authentication wherever possible.

Explain Kerberos.

Kerberos is a computer-network authentication protocol that works on the basis of tickets to allow systems to prove their identity to one another in a secure manner.

Here are the most basic steps taken to authenticate in a Kerberized environment.

1. Client requests an authentication ticket (TGT) from the Key Distribution Center (KDC)
2. The KDC verifies the credentials and sends back an encrypted TGT and session key
3. The TGT is encrypted using the Ticket Granting Service (TGS) secret key
4. The client stores the TGT and when it expires the local session manager will request another TGT (this process is transparent to the user)

If the Client is requesting access to a service or other resource on the network, this is the process:

5. The client sends the current TGT to the TGS with the Service Principal Name (SPN) of the resource the client wants to access
6. The KDC verifies the TGT of the user and that the user has access to the service
7. TGS sends a valid session key for the service to the client
8. Client forwards the session key to the service to prove the user has access, and the service grants access.

If budget is not a concern how do you secure a web server?

If budget is not a concern a web server can be secured by deploying the following technologies

Network Security

- Anti-DDOS technology
- Firewall (To block traffic on unnecessary ports)
- Intrusion Prevention System
- Web Application Firewall

Host Security

- Antivirus
- HIPS/Host Firewall
- Application control (To restrict the processes running)

Apart from these preventive technologies, we should implement System Hardening and also enable log monitoring on the Web servers.

Also, the web application should be thoroughly tested by application penetration testing methods.

What do you understand by compliance in Cybersecurity?

A compliance framework is a structured set of guidelines that details an organization's processes for maintaining its cyber security.

There are industry specific compliances like:

PCI-DSS	– To protect credit card data. (Banks and E-commerce)
HIPAA	– To protect patients health information. (Hospitals and Insurance companies)
SOX	– Public listed companies
GDPR	– European companies and business that run in European countries.

Hackers and their motivation

Different types of Hackers

- **White Hat Hackers**
  - White hat hackers are authorized hackers who work for the government and organizations by performing penetration testing and identifying loopholes in their cybersecurity.
- **Black Hat Hackers**
  - Black Hat Hackers are hackers who hack for malicious intentions. Like financial gains.
- **Grey Hat Hackers**
  - Gray hat hackers fall somewhere in the category between white hat and black hat hackers. They are not legally authorized hackers. They work with both good and bad intentions; they can use their skills for personal gain.
- **Script Kiddie**
  - A Script kiddie is an unskilled person who uses scripts or downloads tools available for hacking provided by other hackers.
- **Hacktivist**
  - Hacktivist is a hacker or a group of anonymous hackers who gain unauthorized access to government's computer files and networks for further social or political ends.
- **State/Nation Sponsored Hackers**
  - State or Nation sponsored hackers are those who are appointed by the government to provide them cybersecurity and to gain confidential information from other countries to stay at the top or to avoid any kind of danger to the country.
- **Malicious Insider or Whistleblower**
  - A malicious insider or a whistleblower could be an employee of a company or a government agency who gains access/knowledge of inside operations which he speculates to be illegal and threatens to go public.

Few Random questions.

If you had to both compress and encrypt data during a transmission, which would you do first?

- Compress first (to reduce the size) and then Encrypt. Encryption on more data will take longer time.

Between TLS and SSL, which is more secure?

- TLS. SSL is the predecessor of TLS

What is Zeroday?

- A vulnerability or a malware that has be identified but doesn’t have a fix (patch or signature) yet. It is the time period between a vulnerability/malware being identified and release of patch/signature.

Difference between VA and PT.

- Vulnerability Assessment is a process of identifying the vulnerabilities in a system or network.

Penetration Testing is to go one step ahead of identifying the vulnerabilities and exploit the vulnerability.

anand guru

SOC EXPERTS

Interview Questions on **Cyber Attacks**

Anand Guru

Security+ | CySA+ | CEH | ECIH

Founder

SOC Experts

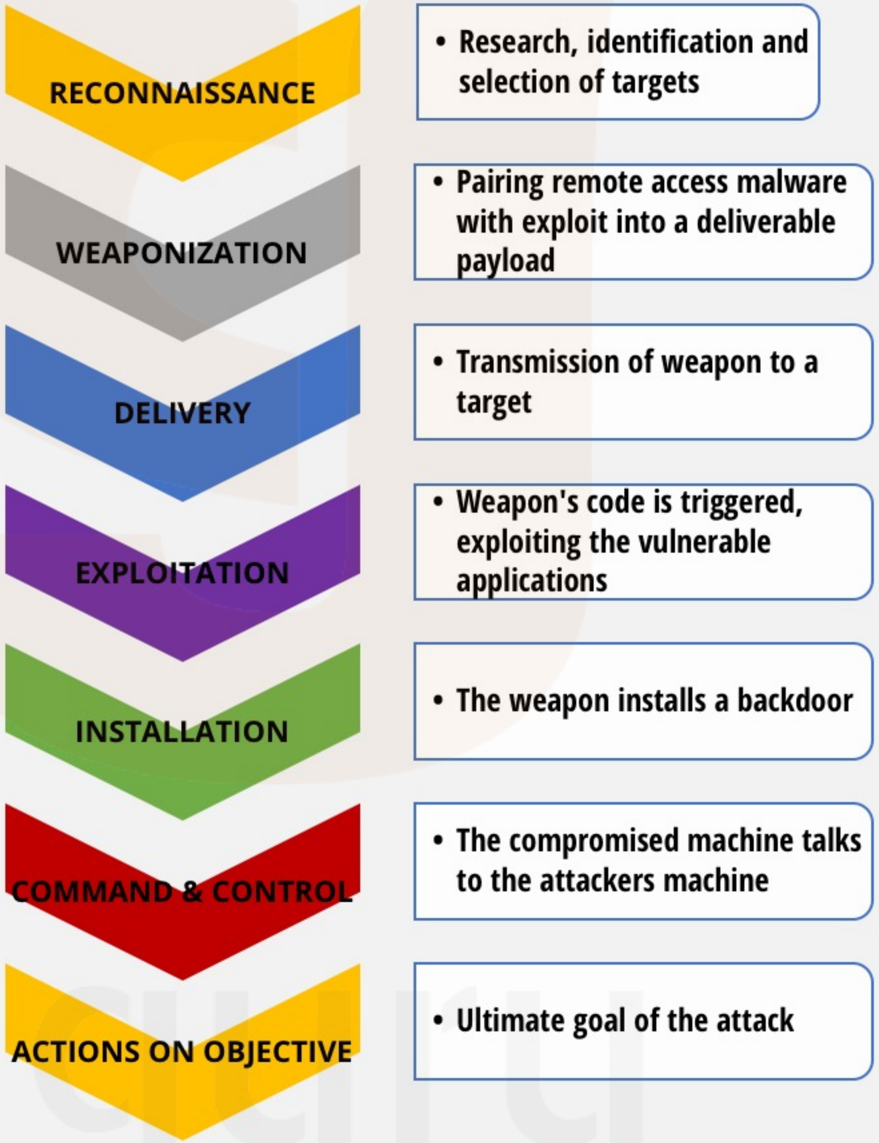
https://socexperts.com

What is Cyber Kill Chain?

Cyber Kill Chain defines the steps used by an attacker to launch and carry-out a cyber attack.

It is defined by **Lockheed Martin**

It has **7 phases**



RECONNAISSANCE

- Research, identification and selection of targets

WEAPONIZATION

- Pairing remote access malware with exploit into a deliverable payload

DELIVERY

- Transmission of weapon to a target

EXPLOITATION

- Weapon's code is triggered, exploiting the vulnerable applications

INSTALLATION

- The weapon installs a backdoor

COMMAND & CONTROL

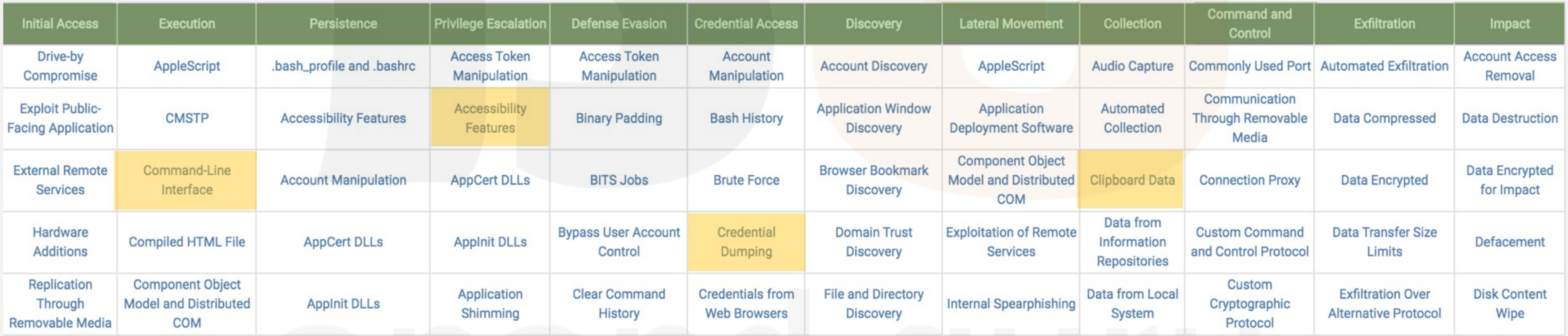
- The compromised machine talks to the attackers machine

ACTIONS ON OBJECTIVE

- Ultimate goal of the attack

What is MITRE ATT&CK Framework?

- The **MITRE** ATT&CK framework is a comprehensive matrix of **tactics** and **techniques** used by threat hunters, red teamers, and defenders to better classify attacks and assess an organization's risk.
- It highlights 12 Tactics and more than 250 Techniques that attackers use



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe

What are TTPs?

TTPs stand for Tactics, Techniques and Procedures

TTPs are patterns of activities or methods associated with a specific threat actor or group of threat actors.

What is Zeroday?

A vulnerability or a malware that has be identified but doesn’t have a fix (patch or signature) yet.

It is the time period between a vulnerability/malware being identified and release of patch/signature.

What is an exploit and payload?

Exploit is a tool that takes advantage of a vulnerability. Usually exploit is used to penetrate into a system taking advantage of an existing vulnerability.

Example – EternalBlue that took advantage of SMB vulnerability

Payload is the actual malware. Part of the malware that does the damage (deleting files, stopping services, encrypting files, gathering and sending sensitive information, taking pictures etc.)

Example – WannaCry used EnternalBlue as exploit and had the ultimate intention of encrypting the files and demand ransom.

Explain Brute-force attack.

Brute-force is a password guessing attack. It tries various combinations of usernames and passwords again and again until it gets in.

Mitigation:

- Encourage users to use complex passwords
- Lockout accounts after few attempts
- Use Captcha to slow down brute-force
- Use multifactor authentication

Explain Dictionary attack.

Dictionary attack is type of brute-force attack. It uses a list of words in a dictionary as passwords.

Dictionary attack can also be personalized by using details of the target like date of birth, spouse name, children name, vehicle number etc.

Mitigation:

- Advise users not to keep a simple word or easily identifiable information as password.
- Encourage users to use complex passwords
- Lockout accounts after few attempts
- Use Captcha to slow down brute-force
- Use multifactor authentication

Explain Rainbow attack.

Rainbow attack is a type of brute-force attack that uses pre-computed password hashes. i.e. instead of trying to pass the password, it tries to match the hash in the user database.

Mitigation:

- Rainbow table attacks can easily be prevented by using salt techniques,
    - **Salt** is a random data that is passed into the hash function along with the plain text.
- Lockout accounts after few attempts
- Use Captcha to slow down brute-force
- Use multifactor authentication

What is Pass-the-hash attack

Pass the hash is a hacking technique that allows an attacker to authenticate to a remote server or service by using the underlying hash of a user's password, instead of requiring the associated plaintext password as is normally the case.

This will reduce the effort of the attacker as he does not have to crack the plaintext password from the stolen hash.

Mitigation:

- Restrict and protect high privileged domain accounts
  - This mitigation reduces the risk of administrators from inadvertently exposing privileged credentials to higher risk computers.
- Restrict and protect local accounts with administrative privileges
  - This mitigation restricts the ability of attackers to use administrative local accounts for lateral movement PtH attacks.
- Restrict inbound traffic using the Windows Firewall
  - This mitigation restricts attackers initiating lateral movement from a compromised workstation by blocking inbound connections on all other workstations with the local Windows Firewall.

What is Scanning?

Scanning is a method for discovering exploitable communication channels.

Scanning for open ports

Scanning for known vulnerabilities

Mitigation:

- Use Firewall and IPS
- OS Hardening
- Use honeypots to detect scanning activities

What is Sniffing Attack?

Sniffing corresponds to theft or interception of data by capturing the network traffic when it flows through a computer network.

Usually done using a packet sniffer

Mitigation:

- Avoid using insecure protocols (like HTTP, FTP, telnet etc. and use secured versions like HTTPS, SFTP, SSH etc.)
- Use encryption whenever possible for data transmission.

What is Spoofing?

Spoofing is a malicious practice employed by cyber scammers and hackers to deceive systems, individuals, and organizations into perceiving something to be what it is not.

Few types of Spoofing

- IP Spoofing
- MAC Address Spoofing
- Email Spoofing
- DNS Spoofing

Mitigation:

- Deploy IPS (IP Spoofing)
- Educate users (Email Spoofing)
- Enable port level security (ARP and MAC Address Spoofing)

Explain Phishing.

- Phishing is a cyber attack that uses disguised email as a weapon.
- The goal is to trick the email recipient into believing that the message is something they want or need
- Example: a request from their bank, for instance, or a note from someone in their company
- Ultimate intention is to get the user to click a link or download an attachment.

Mitigation:

- Use Email Security Solutions (to block obvious phishing and spam emails)
- Educate users
- Use DMARC (Domain-based Message Authentication, Reporting and Conformance)
  - DMARC is a standard for verifying the authenticity of an email. It offers email receivers a way to verify if a message is really from a autorized sender or not.

Other Phishing Attacks

Explain Spear Phishing.

Spear phishing is an email scam targeted towards a **specific** individual, organization or business.

Attackers use the information they have gathered during reconnaissance to make the email appear personalized.

Explain Whaling.

Whaling is a type of phishing that targets senior management/leadership teams/important individuals at an organization

Explain Vishing.

Vishing works similar to phishing, instead of sending and email, the attacker tricks the target to give critical/sensitive information over phone call

Explain DOS and DDOS attack.

Denial-of-Service (DOS) is a type of cyberattack in which the attacker seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services.

Examples:

UDP floods, ICMP floods, SYN floods, fragmented packet attacks, Ping of Death etc.

Distributed Denial-of-Service (DDOS) is a type of attack where multiple systems are used to launch DOS attack on one targeted system.

Usually DDOS are result of multiple compromised systems (called Botnets)

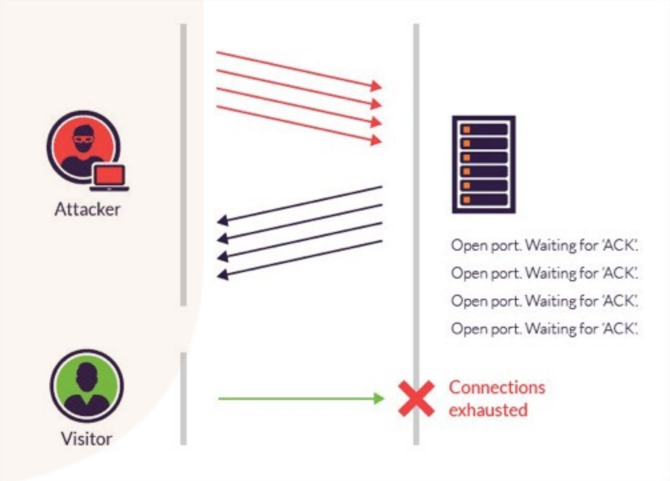
Mitigation:

- Use Anti-DDOS technology (like Arbor)
- Rate limit (limit the number of connections from an IP or User)
- Reduce connection wait time
- Deploy load balancers

Explain SYN flood attack.

SYN Flood attack is a type of DOS attack where it exploits the normal TCP three-way handshake.

The attacker send huge connection requests (SYN) but never sends an acknowledge back to the sever. This will make the server wait for certain time and hold the connection. This will consume all the concurrent connections on the target server making it inaccessible for legit users.


Attacker
Open port. Waiting for 'ACK'.
Open port. Waiting for 'ACK'.
Open port. Waiting for 'ACK'.
Open port. Waiting for 'ACK'.
Visitor
Connections exhausted

Mitigation:

- Use Anti-DDOS technology (like Arbor)
- Rate limit (limit the number of connections from an IP or User)
- Reduce connection wait time
- Deploy load balancers

Explain ARP poisoning.

- Also called as ARP Spoofing
- ARP poisoning is when an attacker sends falsified ARP messages over a local area network (LAN) to link an attacker’s MAC address with the IP address of a legitimate computer or server on the network.
- It is used to do a Man-in-the-Middle attack

Mitigation:

- Use Static ARP
- Detect ARP poisoning using tools like XARP
- Set up Packet filtering
- Install AV and keep signatures updated

Explain MITM attack.

Man-in-the-Middle is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other.

Mitigation:

- Use Static ARP (to prevent ARP poisoning)
- Use Encryption (prevent the attacker from leveraging the data)
- IPS system (can detect sudden change in the network performance)

Explain DNS Poisoning.

- Also called as DNS Spoofing
- Type of cyberattack that exploits vulnerabilities in the domain name system (DNS) to divert Internet traffic away from legitimate servers and towards fake ones.
- This is done by introducing corrupt (poisoned) DNS data into DNS Resolver’s Cache.

Mitigation:

- Regularly audit DNS Zones
- Keeping DNS Servers up-to-date.
- Restrict Zone Transfers
- Limit recursive queries.
- Store only data related to the requested domain.

What is DNS Tunneling?

- DNS Tunneling is a method of cyber attack that encodes the data of other programs or protocols in DNS queries and responses.
- Usually DNS traffic is allowed through firewalls and attackers take advantage of this.
- It is used for data exfiltration (without being detected)

Mitigation:

- IPS Systems can help detect few DNS Tunneling attacks
- Block communication to IPs that are known to be used for data exfilteration
- Use DNS firewall
- Deploy standalone DNS protection solution (Like Infoblox)

What is a malware?

- Malware is a (malicious) software intentionally designed to cause damage to a computer or computer network.
- The malicious activities include

  Deleting files

  Encrypting files

  Gain access of the infected machine

  Collecting and sending sensitive data

  Stopping services

  System shutdown etc.

Mitigation:

- Use AV with up-to-date signature
- Use Ad-blockers
- Educate users not to download files from unknown sources

Explain different Types of Malware.

Virus: Viruses attach themselves to clean files and infect other clean files. Their intention is to damage a system's core functionality and deleting or corrupting files. They usually appear as an executable file (.exe).

Trojans: This kind of malware disguises itself as legitimate software but has malicious intent. It tends to act discreetly and create backdoors in your security to let other malware in.

Worms: Worms infect entire networks of devices, either local or across the internet, by using network interfaces. It uses each consecutively infected machine to infect others.

Spyware: Spyware is malware designed to spy on you. It hides in the background and takes notes on what you do online, including your passwords, credit card numbers, surfing habits, and more.

Ransomware: This kind of malware typically locks down your computer and your files, and threatens to erase everything unless you pay a ransom.

Adware: Though not always malicious in nature, aggressive advertising software can undermine your security just to serve you ads — which can give other malware an easy way in. Plus, they end up consuming system resources

Botnets: Botnets are networks of infected computers that are made to work together under the control of an attacker.

RAT: Remote Access Trojan – Type of malware that allows an attacker gain unauthorized remote access of victim's machine

Difference between Virus and Trojan and Worm?

Virus: Viruses attach themselves to clean files and infect other clean files. A user action (like execution) is required for the virus to run.

Trojans: They appear as useful programs, but have malicious intentions. Trojans are usually used to trick the user into performing certain action (like execution)

Worms: Worm spread in the network without user actions. They spread by

- Attached external storage
- Available open network shares
- Email (a worm can automatically send a copy of itself to all the users in your address book)

What is drive-by-download?

- A drive-by download refers to the unintentional download of malicious code onto a computer or mobile device that exposes users to different types of threats.
- In this type of attack, users need not click on anything to initiate the download. Simply accessing or browsing a website can activate the download.
- Drive-by download happens by taking advantage of insecure, vulnerable, or outdated apps, browsers, or even operating systems.

Mitigation:

- Encourage users to keep their software up to date
- Install AV that is capable of scanning internet traffic
- Install web-filtering software.
- Restrict add-ons on browsers.
- Educate users not to visit untrusted websites.

What is fileless malwares or fileless attack?

- Fileless malware sneaks in without using traditional executable files as a first level of attack.
- Rather than using malicious software or downloads of executable files as its primary entry point onto corporate networks, fileless malware often hides in memory or other difficult-to-detect locations.
- Uses living-off-the-land techniques
- Fileless malware leverages trusted, legitimate processes running on the operating system to perform malicious activities.
- Simply put, fileless malware run on RAM (memory-based) and doesn't have any trace on the Disk (file-based). This makes it impossible for a traditional antivirus which rely on signatures to detect a malware.

Mitigation:

- Use EDR tools to monitor and detect suspicious activities.
- Disable command line shell scripting language, including PowerShell and Window Management instrumentation, wherever it's not needed

What is OWASP?

The Open Web Application Security Project (OWASP) is an online community that produces articles, methodologies, documentation, tools, and technologies in the field of web application security.

Every year OWASP announces List of Top 10 Vulnerabilities for Web Applications – OWASP Top 10

As of 2019, top 10 web application attack/vulnerabilities are:

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XEE)
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting
- Insecure Deserialization
- Using Components With Known Vulnerabilities
- Insufficient Logging And Monitoring

Explain SQL Injection.

SQL injection is a code injection technique in which malicious SQL statements are inserted into an entry field for execution.

These SQL statements control a database server behind a web application. By executing malicious statements, the attacker can gain unauthorized access, copy, modify or delete the data.

Example of malicious SQL Statement: **' OR '1'='1' --**

Mitigation:

- Input validation
- Sanitize all inputs (like remove quotes and special characters)
- Use IPS and WAF solutions
- Turn off visibility of Database errors on production servers

Explain Cross Site Scripting (XSS).

Cross-site Scripting (XSS) is a client-side code injection attack. The attacker aims to execute malicious scripts in a web browser of the victim by including malicious code in a legitimate web page or web application.

Usually happens where there is a text message box in the website. Like comments for a blog.

Mitigation:

- Input validation
- Sanitize all inputs (like remove quotes and special characters)
- Encode data on output.

Explain Cross Site Request Forgery (CSRF).

- Also called as **one-click attack** or **session riding**
- Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated.

Example:

- User A is connected to a banking website – www.mybank.com
- Attacker tricks the user into downloading and executing a code.
- This code will send request to www.mybank.com to transfer money to attackers account.
- In this case the banking website performs the request because it see the request coming from User A's machine who is already authenticated with the server.

Mitigation:

- Synchronizer token pattern
- Cookie-to-header token
- Double Submit Cookie

Explain Broken Authentication.

Broken Authentication weaknesses can allow an attacker to either capture or bypass the authentication methods that are used by a web application.

- Permits automated attacks such as credential stuffing, where the attacker has a list of valid usernames and passwords.
- Permits brute force or other automated attacks.
- Permits default, weak, or well-known passwords, such as "Password1" or "admin/admin“.
- Uses weak or ineffective credential recovery and forgot-password processes.
- Uses plain text or weakly hashed passwords

Mitigation:

- Where possible, implement multi-factor authentication to prevent automated, credential stuffing, brute force, and stolen credential re-use attacks.
- Do not ship or deploy with any default credentials, particularly for admin users.
- Implement weak-password checks, such as testing new or changed passwords against a list of the top 10000 worst passwords.
- Lock user accounts after certain failed attempts

Explain Broken Access Control.

Broken Access Control is a weakness in web application that will let the users do more than what they are authorized. Example, user A can see the details of user B.

Broken Access Control vulnerabilities often lead to

- unauthorized information disclosure
- modification or destruction of all data
- performing a business function outside of the limits of the user.

Mitigation:

- Deny access to functionality by default.
- Use Access control lists and role-based authentication mechanisms.
- Log access control failures, alert admins when appropriate (e.g. repeated failures).

Interview Questions on

SOC Processes

Anand Guru

Security+ | CySA | CEH | ECIH

Founder

SOC Experts

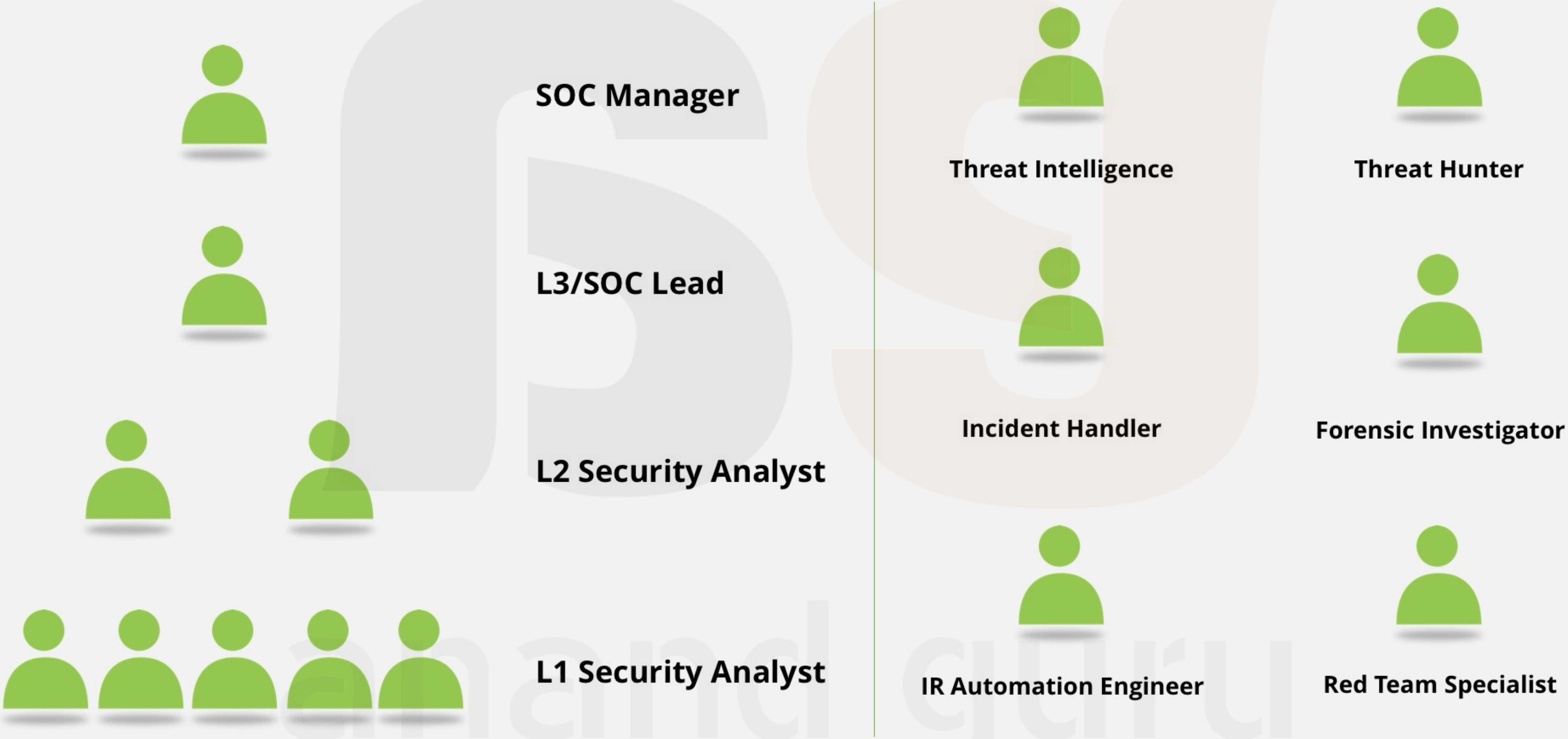
https://socexperts.com

anand guru

DISCLAIMER

- **Most of the questions and their answers discussed in this section are subjective.**
- **Different companies follow different processes.**
- **I believe there are no correct or wrong answers for these questions. However there might be better answers than the ones discussed here.**

Explain the SOC Team Architecture/Hierarchy



SOC Manager

L3/SOC Lead

L2 Security Analyst

L1 Security Analyst

Threat Intelligence

Threat Hunter

Incident Handler

Forensic Investigator

IR Automation Engineer

Red Team Specialist

Roles and Responsibilities of L1/L2 Security Analyst in SOC.

Security Analyst L1

- 24/7 Eyes-on-Glass monitoring
- Analysis of triggered alerts (usually following a Runbook)
- Raising tickets for validated incidents
- Follow-up with incident response team for remediation
- Drafting shift hand-overs
- Assist L2/L3 in reporting

Security Analyst L2

- Deep dive analysis of escalated alerts
- Assist in Incident Remediation
- Assist L1 in alert analysis
- Maintaining and improving SOPs and processes
- Troubleshoot basic SIEM issues

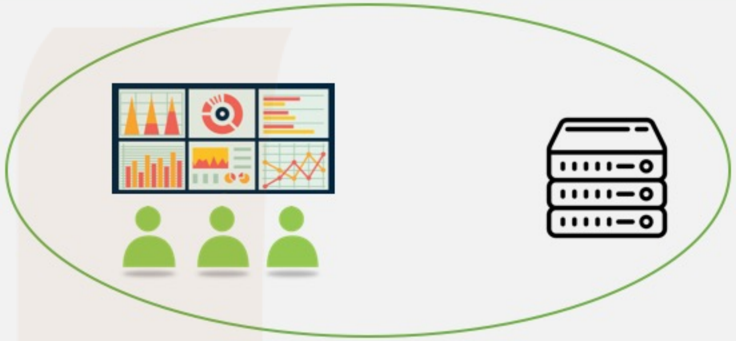
As SOC Lead/SIEM Admin what are your responsibilities?

1. Installing, updating, upgrading SIEM solution.
2. On-boarding log sources and working on log source issues.
3. Create and fine-tune content in SIEM – Correlation Rules, Dashboards, Reports, Lists etc.
4. Interact with SIEM vendor TAC (support) to fix any issues with SIEM.
5. Install, Manage and build content in SIEM.
6. Mentor L1 and L2 security analyst.
7. Assist in analysis that requires involvement of multiple teams.
8. Evaluate new solutions for SOC team.
9. Create Run books for all alerts.
10. Schedule shift rooster.

What are the different SOC Models?

- ## In-house SOC

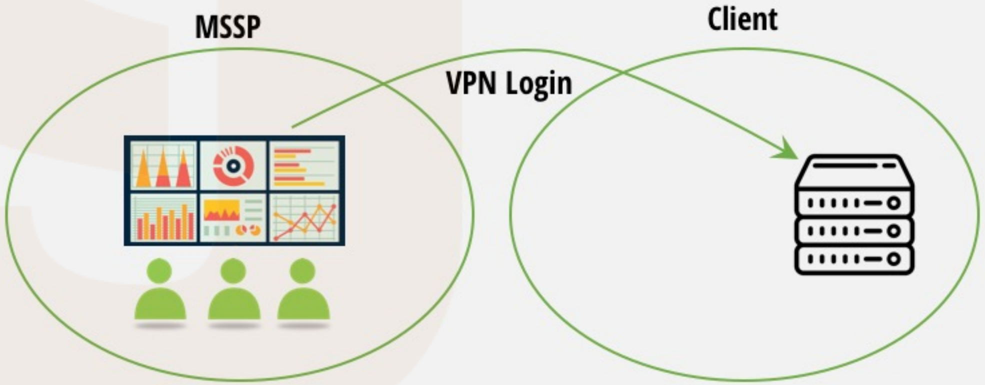
  An organization runs its own SOC. People, processes and technology are all managed by people with-in the organization.



- ## MSSP (Managed Security Service Provider)/ MSP (Manager Security Provider)

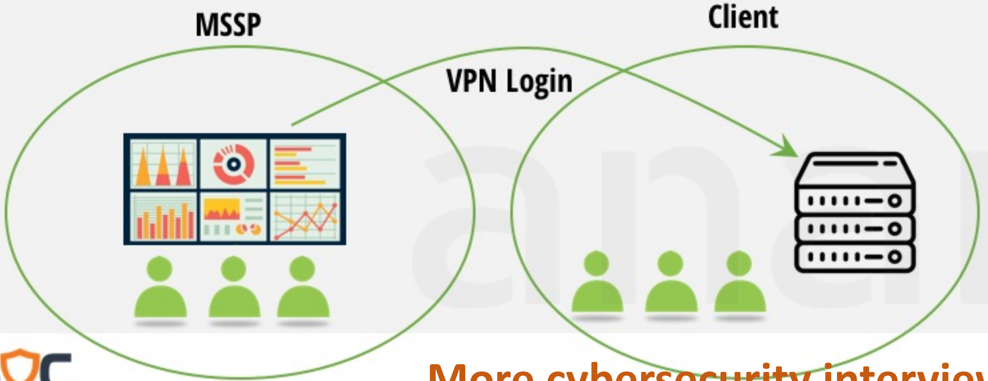
  Dedicated – A team of people with the service provider work for a client. Here the client typically have their own technology i.e. SIEM and other tools will be hosted in clients datacenter.

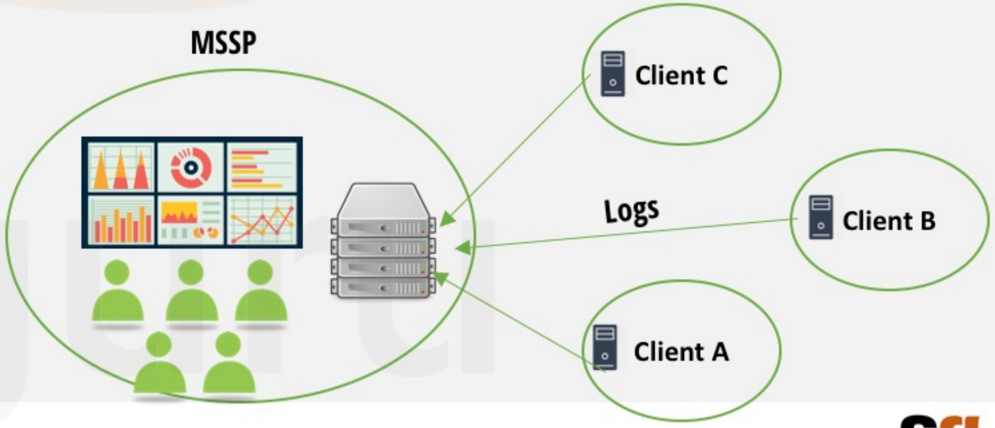
  Shared – A team of people with the service provider monitor and analyze logs coming from various clients. In this model the technology is hosted on service providers datacenter



- ## Hybrid SOC

  It is a mix of both In-house SOC and MSSP. Typically this is done by out-sourcing the L1 monitoring to a MSSP and the organization runs L2 and Incident Response team in-house





Which model is better MSSP or In-house?

Both the models have their advantages and short comings

In-house SOC is more effective as the organizations can customize everything as per business requirements. Since the number of technologies in an organization is limited, the focus will be on getting best value out of each solution. However, in-house SOC is very expensive to implement

MSSP model will reduce the cost of ownership and operational expenses; however, the output of SOC (like reports, alerts, recommendation etc.) will be generic.

Hybrid SOC gives a better result, but it is still expensive to implement.

What is SLA?

- SLA stands for Service Level Agreement
- In SOC it is mostly the time taken for a SOC team to identify and report a suspicious activity.
- SLAs are associated with priorities:

P1	**30 minutes**
P2	**1 hour**
P3	**2 hours**
P4	**4 hours**

Why does a organization need SOC team?

- One of the main benefits of having a Security Operations Center is that it improves security incident detection through constant monitoring and analysis.
- It shifts to proactive approach, rather than being reactive.
- Monitoring 24/7, a SOC is able to provide organizations with an advantage to defend against intrusions regardless of the type of attack at any time.
- SOC also helps to meet the regulatory compliances

When we have Endpoint Security and Network Security, why do we need SOC team?

- Traditionally all the preventive technologies (like AV, firewall, IPS) work separately and needs dedicated skills to manage them. A SOC team helps in **correlating** activities happening at different parts of the network.

What do you document in an Incident?

1. Incident Name
2. Incident Description
3. Priority
4. Occurred Time
5. Detected Time
6. Reported By
7. Assigned To
8. Affected Host/IP/User/Business Unit
9. Information Gathered
10. Analysis
11. Evidence
12. Recommendations

What ticketing tool have you worked on?

Most widely used ticketing tools are

- Service Now (SNOW)
- BMC Remedy
- JIRA
- RSA Archer

Apart from SIEM what other tools have you worked on?

Preventive Technologies

- **Endpoint Security – McAfee ePO or SEPM**
- **Firewall – PaloAlto or Fortinet**
- **IPS – SNORT**
- **Vulnerability Assessment - Nessus**
- **Proxy – Websense**
- **Email Gateway – Proofpoint**
- **WAF – Imperva Incapsula**

Analysis Tools

- **IPVOID**
- **VirusTotal**
- **Wireshark**
- **MXToolBox**
- **CVEDETAILS**
- **US-CERT**
- **IBM X-Force/Threat Crowd**

Utility Tools

- **Ticketing tool – Service NOW**
- **Process Explorer**
- **Process Monitor**

What is False Positive?

- A **true positive** is an outcome where the model *correctly* predicts the *positive* case.
  - Downloaded file is a malware, AV detected it as malware
- A **true negative** is an outcome where the model *correctly* predicts the *negative* case.
  - Downloaded file is NOT malware, AV did NOT detect it as malware
- A **false positive** is an outcome where the model *incorrectly* predicts the *positive* case.
  - Downloaded file is a NOT a malware, AV detected it as malware
- A **false negative** is an outcome where the model *incorrectly* predicts the *negative* case.
  - Downloaded file is a malware, AV did NOT detect it as malware

- True Positive and Ture Negative are ideal cases; i.e. when solutions are working correctly
- False Positive – Increases work and lead to alert-fatigue
- False Negative – Is very dangerous; malicious activity has happened, solution did not detect it.

Explain your team in numbers and Hierarchy

- We have 10 people in our team with
  - 6 Level 1 Analyst
  - 2 Level 2 Analyst
  - 1 Lead &
  - 1 SOC manager
- Our team reports to CISO in our company (or client's CISO)
- L1 analysts monitors network 24/7 and do analysis based on the Playbooks
- L2 analysts helps in deep dive analysis and also assist L1s in analysis.
- Threat Intelligence and Threat Hunting responsibilities are shared between L1 and L2 analyst

What are the numbers in your SOC?

No. of Log Source	- Around 2800
No. of Logs/day	- 25,000,000
No. of Alerts/day	- 100 – 130
No. of Incidents/day	- 2 – 5

What are the different report/dashboard you generate?

3 major types of reports - Technology Report | SIEM Performance Reports | SOC Performance Report

Technology Reports

1. Malware Summary
   - No. of Infections, Hosts Infected, Users, Malware Type, Malware Name, Action by AV, File Name and File Path
2. Firewall Summary
   - Inbound Allow – Source Country, Source IP, Destination IP, Destination Port (services)
   - Inbound Deny – Source Country, Source IP, Destination IP, Destination Port (services)
   - Outbound Allow – Source IP, Destination IP, Destination Country, Destination Port (services)
   - Outbound Deny – Source IP, Destination IP, Destination Country, Destination Port (services)
3. Account Management Summary
   - Accounts Created, Deleted, Enable, Disabled, Locked-out
   - Privilege Changes
4. Authentication Summary
   - Successful logons, Failed Logons, Admin Logons etc.
5. Proxy Summary
   - Top 10 Users, Top 10 Websites, Top 10 Website Categories, Malicious Website Access and Action, Malicious file downloads and Action
6. Email Summary
   - Top 10 Sender, Top 10 Recipients, Top 10 Sender Domain, Top 10 Mail blocking Reasons, Malicious Attachment and Action
7. Threat Intelligence Summary
   - Inbound – Source country, Source IP, Destination IP, Destination Port, Action
   - Outbound – Source IP, Destination IP, Destination Country, Destination Port, Action

Reports contd...

SIEM Reports

- EPS
- New log sources
- Silent log sources
- New Correlation Rules

SOC Performance Reports

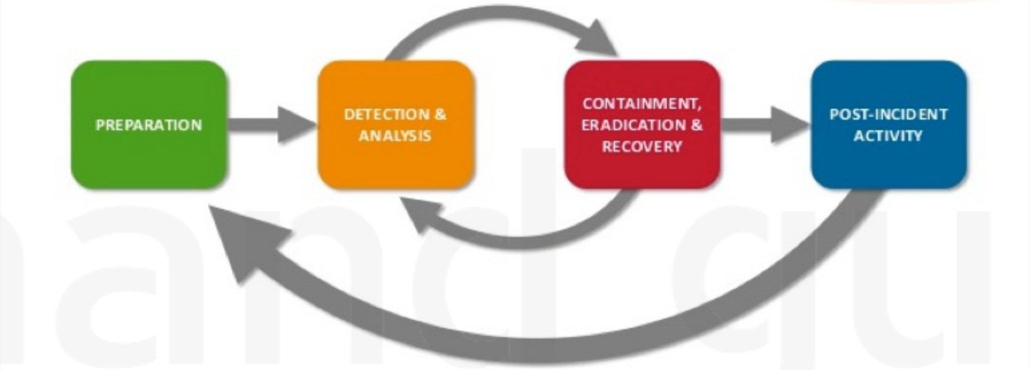
- Number of Alerts
- Number of Incidents by Severity
- SLA adherence
- Number of Escalation

Explain the Incident Response Process/Lifecycle

SANS (SysAdmin, Audit, Network and System) Incident Response Process has 6 stages

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

NIST (National Institute of Standards and Technology) defines the Incident Response in the **Special Publication 800-61**



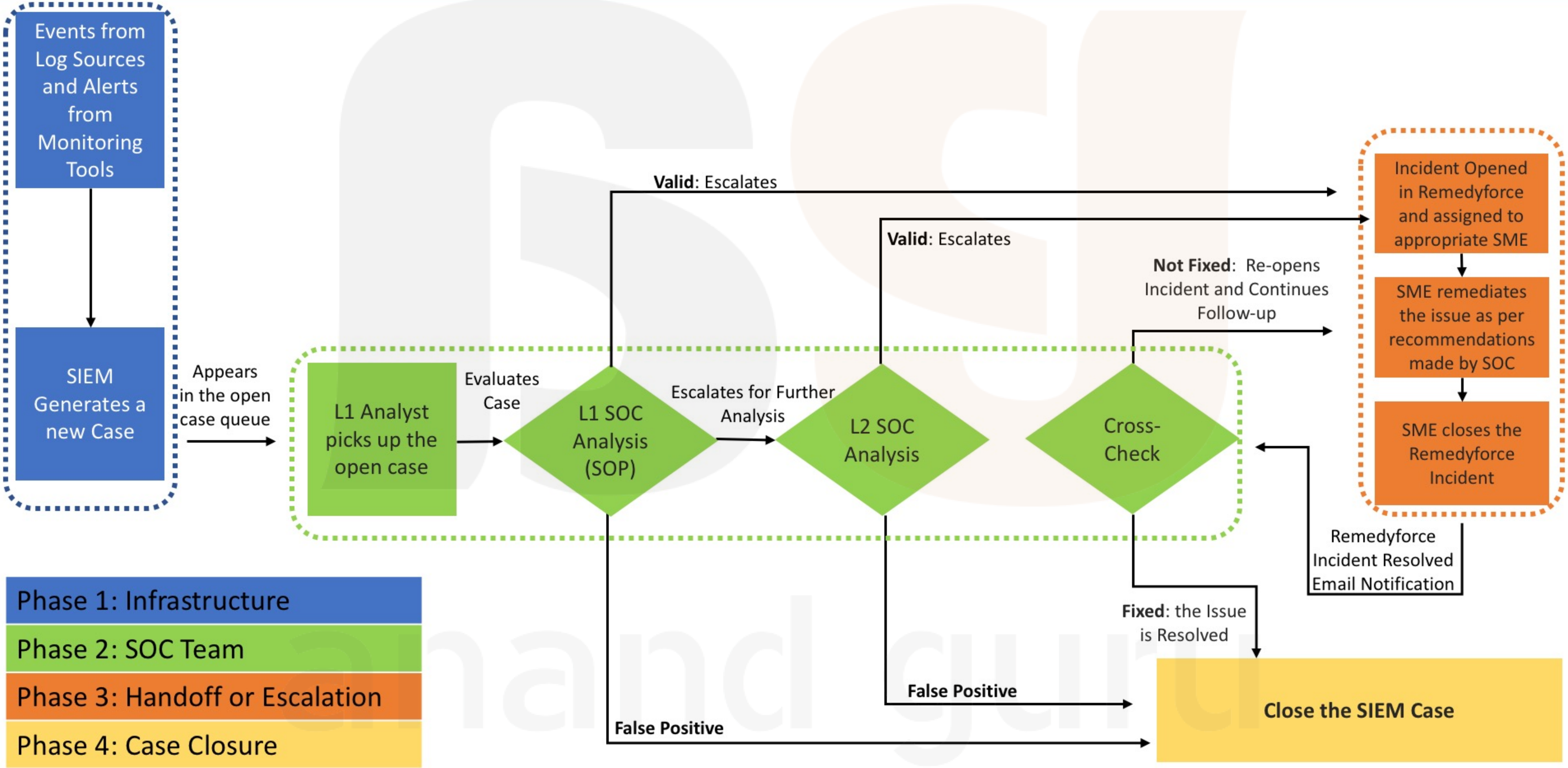
Explain SIEM implementation Phases.

1. Asset Management (List of all the assets)
2. Define the Scope for SOC Monitoring and Analysis
3. Log Source On-boarding preparation
4. Implement SIEM
5. On-board Log sources
6. Use OOB content – DB, Reports, Rules etc.
7. Announce Go Live
8. Analysts start getting comfortable with the tools.
9. Create Custom content as per requirement

Explain SOC Implementation Phases.

1. Define Scope
2. Implement Technologies
3. Hire and Build Team
4. Develop Policies, Processes and Procedures
5. CMM Level 3 (Initial – Managed -- Defined State)
6. Develop KPIs – (Quantitatively Managed)
7. Automate – (Optimized)

Explain SOC Workflow.



Events from Log Sources and Alerts from Monitoring Tools

SIEM Generates a new Case

Appears in the open case queue

L1 Analyst picks up the open case

Evaluates Case

L1 SOC Analysis (SOP)

Valid: Escalates

Escalates for Further Analysis

L2 SOC Analysis

Valid: Escalates

Cross-Check

Not Fixed: Re-opens Incident and Continues Follow-up

Incident Opened in Remedyforce and assigned to appropriate SME

SME remediates the issue as per recommendations made by SOC

SME closes the Remedyforce Incident

Remedyforce Incident Resolved Email Notification

Fixed: the Issue is Resolved

False Positive

False Positive

Close the SIEM Case

Phase 1: Infrastructure

Phase 2: SOC Team

Phase 3: Handoff or Escalation

Phase 4: Case Closure

What metrics do you use in SOC?

KPI	Why Do We Care?	Possible Measurements	Assessment of...
Number of devices being monitored	· How many devices are being monitoring? · Is the number increasing or decreasing? Why?	· Number of devices · Number of devices / analyst	· Workload
Total number of events	· How many events are being handled? · Is the number increasing or decreasing? Why? · Are the current staffing levels adequate?	· Number of events / hour (/ analyst) · Number of events / day (/ analyst) · Number of events / month (/ analyst) · Number of events / year (/ analyst) · Number of events / event type	· Cost to value · Key risks · Workload
Number of events per device or host	· How many events are received for each device or host? · Are there certain devices or hosts which are more prone to security issues, causing increased risk? Why? · Are there certain devices or hosts which are more prone to false positive events? Why?	· Number of events per device or host/day · Number of events per device or host/month · Number of events per device or host/year · Number of events / device or host type · Number of events / operating system type	· Detection success · Key risks
Number of events per location	· How many events are received per geographic location, office, etc.? · Are certain locations more prone to security events? Why?	· Number of events / department · Number of events / office · Number of events / region	· Key risks
Number of false positive alerts	· How many false positive events are received? Is this acceptable? · Can the number of false positive events be reduced? How?	· Number of false positives / hour · Number of false positives / day · Number of false positives / month · Number of false positives / year · Percentage of events that are false positives	· Detection success
Time to detection	· How long is it taking your organization to detect a security event? Is this acceptable? · Are there ways this time to detection can be reduced? How?	· Measured in minutes, hours or days... · Average time to detection · Average time to detection / technology · Average time to detection / event type · Outliers	· Detection success · Process success
Time to resolution	· How long is it taking our organization to resolve an actual security event? Is this acceptable? · Are there process or technology improvements that can be made to reduce this time? What are they? · Are additional staff or training required? How many staff or what additional training is required?	· Measured in minutes, hours or days... · Average time to identify · Average time to identify / technology · Average time to identify / event type Outliers	·Analyst skills ·Process success
Escalation level	· How many events are being escalated and to what level? · Are events being escalated too quickly or not soon enough? Why? · Are there improvements to the escalation process that can make event handling more efficient? What are they? · Is the training for each level sufficient to produce the desired skill level? If not, what additional training is required?	· Average number of events / level · Average number of events / level / (time period) · Escalation level / event type · Escalation level / technology · Average time (min or hours) to escalate	· Analyst skills · Cost to value · Process success

More cybersecurity interview questions & answers @ https://bit.ly/ag-soc-qna

What do you document in Shift Handover?

Items	Comments
Shift Start Time	18 Feb 2020 | 6:00 AM
Shift End Time	18 Feb 2020 | 15:00 PM
Any on-going issues?	Any alert analysis pending? Any teams waiting for update from SOC team?
Incident Details	Incident raised during the shift • Incident Number • Incident Name & Description • Severity • Assigned to (Team) • Status
Task Handover	Reports to pull

Difference between Blueteam vs Redteam.

Red team is a responsible for offensive security. Typically they do penetration testing, exploiting vulnerabilities, social engineering and various recon activities

Blue team is a responsible for monitoring, detection and responding to a possible threat.

A team that does both Red team and Blue team activities is called a Purple Team

What documents do you create in SOC?

Log Source On-boarding

Log Source Decommissioning

Threat Intel gathering procedure

Threat Hunting methodologies

New Use case development procedure

Staff on-boarding procedure

Play-book/Run-book (Investigation Procedures)

Data/Config backup Procedure

What is SOP/ RunBooks/ PlayBooks?

A step-by-step guide to handle an alert in Security Operation Center

Usually followed by L1 Security Analyst

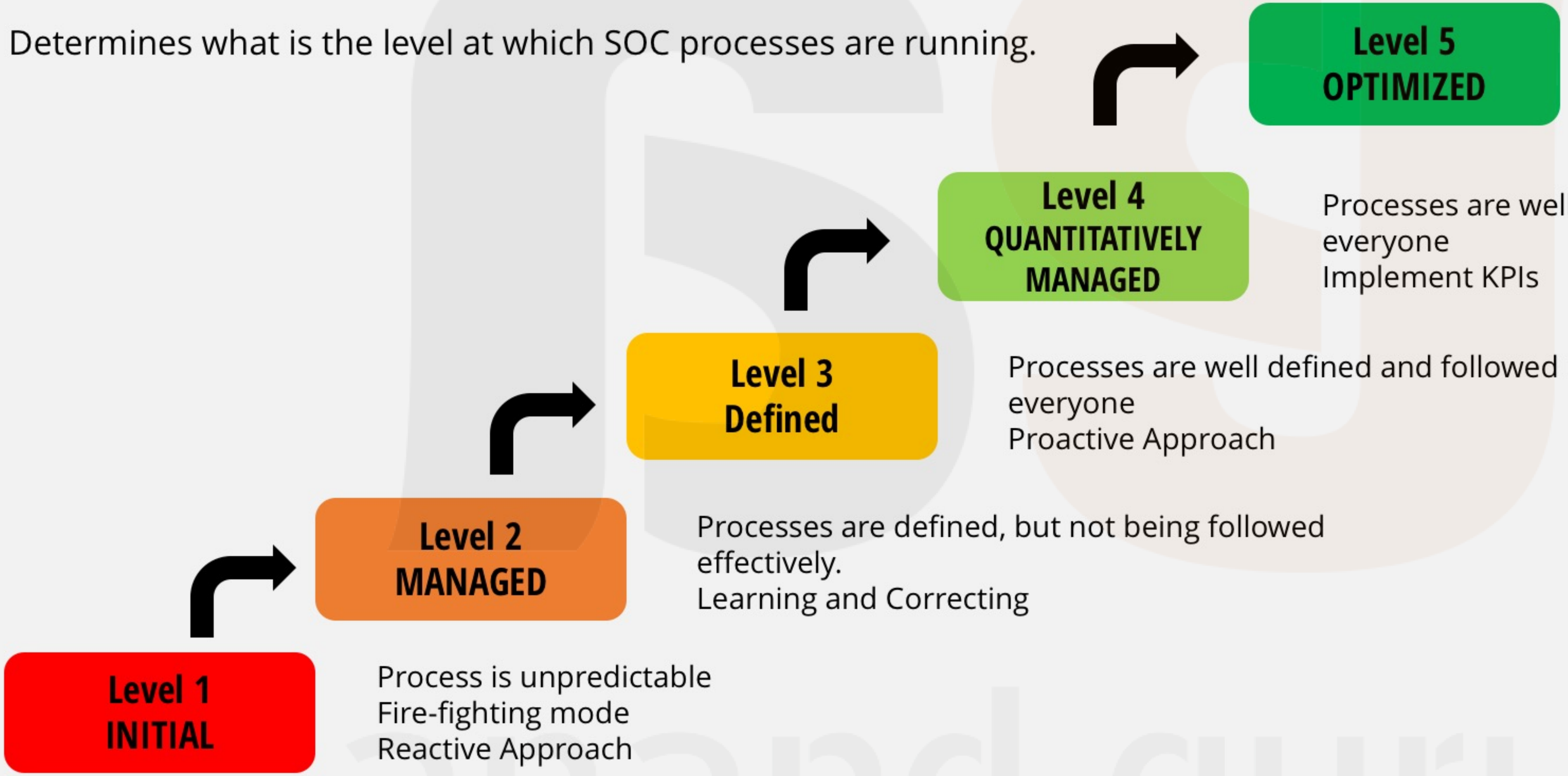
This helps in maintaining the quality of analysis and incident documentation

SOPs also reduce the time to respond

Explain CMM level as applied to SOC.

CMM stands for Capability Maturity Model

Determines what is the level at which SOC processes are running.



Level 1 INITIAL

Process is unpredictable
Fire-fighting mode
Reactive Approach

Level 2 MANAGED

Processes are defined, but not being followed effectively.
Learning and Correcting

Level 3 Defined

Processes are well defined and followed by everyone
Proactive Approach

Level 4 QUANTITATIVELY MANAGED

Processes are well defined and followed by everyone
Implement KPIs

Level 5 OPTIMIZED

Automate repetitive tasks
Improve quality and performance

How do you handle a P1 incident in your SOC?

- In our organization, the SLA for P1 incident is 30 minutes.
- We have an internal process of involving SOC Lead within first 10 minutes of a P1 alert.
- Lead will take a call of which other teams assistance could be required.
- Open a bridge call and all the stake holders will be notified about the incident.
- I continue to provide the assistance to the lead by pulling reports or checking the status of affected services etc.

What will you do if there are 200 alerts triggered at once?

- If there are so many alerts, it is most likely possible that the same alert has triggered several times.
- So I will isolate the duplicate alerts.
- If there are different alerts, I will sort them by priority and pick the one with high priority and impact.
- If the triggered alerts are for a new correlation rule, it is possible that it is configured incorrectly. I will pass this information to the SIEM Engineer for fine-tuning.

What do you discuss in client calls?

- We have weekly call with the customer
- We discuss things like
  - Incident Trends
  - Threat Indicators Summary
  - SLA Report and KPIs
  - SIEM Health Report
    - EPS
    - New log sources
    - Silent log sources
    - New Correlation Rules

Interview Questions on
Logs (Raw Logs)

Anand Guru

Security+ | CySA+ | CEH | ECIH

Founder

SOC Experts

https://socexperts.com

What are the different logging levels in network devices?

Most network device have the following logging levels

- Level 0 —**Emergency** : System unusable
- Level 1 — **Alert** : Immediate action needed
- Level 2 — **Critical** : Critical condition—default level
- Level 3 — **Error** : Error condition
- Level 4 — **Warning** : Warning condition
- Level 5 — **Notification** : Normal but significant condition
- Level 6 — **Informational**: Informational message only
- Level 7 — **Debugging** : Appears during debugging only

What are the important logs in Windows Server?

Windows Event Logs are the most important logs in Windows servers.

There are 3 main categories in Windows Event Logs

- **Application**
- **System**
- **Security**

Default location of logs for few log sources.

Windows Event Logs	: C:\WINDOWS\system32\config\
Windows DHCP	: C:\Windows\System32\DHCP
Windows DNS	: **(Trick Question)** By default DNS logging is not enabled. When we enable we get an option to choose the log file path
Linux System	: /var/log/messages
Exchange Mail Server	: %ExchangeInstallPath%\TransportRoles\Logs\MessageTracking NOTE: Important logs in Exchange are Message Tracking logs

Can you recall few Event IDs of Windows Event Logs?

1. 4624 – Successful User Account Login
2. 4625 – Failed User Account Login
3. 4720 – A user account is created
4. 4726 – A user account was deleted
5. 4740 – A user account was locked out
6. 4767 – A user account was unlocked
7. 1102 – The audit log was cleared

What are Windows Logon Types?

The logon type field indicates the kind of logon that occurred.

- **Logon Type 2 – Interactive**
- **Logon Type 3 – Network**
- **Logon Type 4 – Batch**
- **Logon Type 5 – Service**
- **Logon Type 7 – Unlock**
- **Logon Type 8 – NetworkCleartext**
- **Logon Type 9 – NewCredentials**
- **Logon Type 10 – RemoteInteractive**
- **Logon Type 11 – CachedInteractive**

Logon type 2, 3 & 10 are the most common type of logons

What are the reasons for Login failures in Windows?

Status and Sub Status Codes	Description
0xC0000064	User name does not exist
0xC000006A	User name is correct but the password is wrong
0xC0000234	User is currently locked out
0xC0000072	Account is currently disabled
0xC000006F	User tried to logon outside his day of week or time of day restrictions
0xC0000070	Workstation restriction, or Authentication Policy Silo violation
0xC0000193	Account expiration
0xC0000071	Expired password
0xC0000133	Clocks between DC and other computer too far out of sync
0xC000015B	The user has not been granted the requested logon type (aka logon right) at this machine

What are the important fields in antivirus logs?

Date & Time	- 18 Feb 2020 10:10:48
Host	- LJOHN0708
IP Address	- 10.10.2.78
User	- ABCInsurance\john
File Name	- goodmovie.exe
File Path	- D:\Movies\New Folder\goodmovie.exe
Malware Name	- Every vendor has their naming conventions
Malware Category	- Trojan, Worm, Ransomware etc.
Action Taken by AV	- Clean, Delete, Quarantine, Failed to Clean, Failed to delete, Failed to Quarantine

What are the important fields in firewall logs?

- Date & Time
- Source IP
- NAT Source IP
- Source Port
- Source Interface/Zone
- Destination IP
- NAT Destination IP
- Destination Port
- Destination Interface/Zone
- Rule Name
- Action
- Bytes Sent
- Bytes Received
- Source Country
- Destination Country

What are the important fields in IPS logs?

Date & Time

Source IP

Source Port

Destination IP

Destination Port

Attack Name

Attack Severity

Source Country

Destination Country

Action

What are the important fields in proxy logs?

Date & Time

Source IP

User

URL

Domain

Website Category

Action

Bytes Sent

Bytes Received

What are the important fields in WAF logs?

Date & Time

Client IP

Request Headers

Response Headers

URL

Referrer

Method

HTTP Status Code

Attack Type

Attack Severity

What logs do you pull from AWS?

AWS CloudTrail Logs

AWS CloudWatch Logs

How do you pull logs from AWS?

Using AWS API.

We would need the **Access key** and **Secret access key** of a user account. This user should have permission to read logs form S3 buckets.

What logs do you collect from a database?

Audit Logs

Why do we need raw logs?

- The raw logs are required for Forensics and Compliance purposes.

Difference between Flows and Events.

- **Event** is a log of a particular action.
- A **flow** records information like number of packets, bytes sent, bytes received and connection time.

Difference between an Event, Alert and Incident

- **Event** is a log of particular action on a server.
- **Alert** is a suspicious (not confirmed) activity in the network.
- An **incident** is a confirmed malicious activity.

Interview Questions on **SIEM**

Anand Guru

Security+ | CySA+ | CEH | ECIH

Founder

SOC Experts

https://socexperts.com

What is SIEM?

SIEM stands for Security Information and Event Management.

It is security management solution that helps in collecting, parsing and correlating events from various log sources

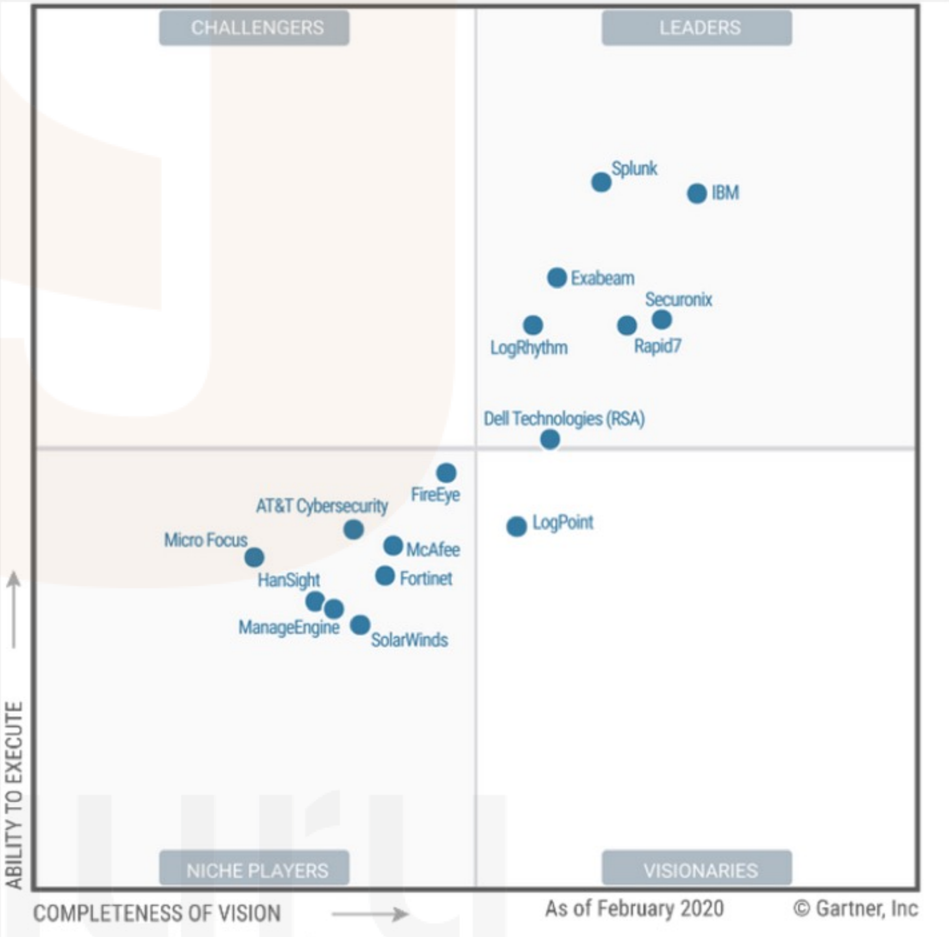
Why do we need SIEM?

When we have security solutions like AV, Firewall, IPS why do we need SIEM?

- Various security solution that we use to protect our network and data work in isolation.
- However, in order to detect todays sophisticated attacks, it would be helpful if we could correlate information from various devices. This correlation is provided by SIEM.
- AV, F/W, IPS are all preventive technologies where as SIEM is mostly used for detection and analysis.
- We need SIEM for regulatory compliances too.

What are the popular SIEM vendors?

- According to Gartner's Magic Quadrant the leaders in SIEM market are
  - ✓ Splunk Enterprise Security
  - ✓ IBM QRadar
  - ✓ Exabeam
  - ✓ Securonix
  - ✓ LogRhythm
  - ✓ RSA Security Analytics
- Other popular SIEM include
  - ✓ Microfocus Arcsight



Source: Gartner (February 2020)

What is Parsing?

- Parsing is process of converting unstructured data into structured format.
- It is during parsing where SIEM extracts all the useful metadata like Source IP, Destination IP, Username, File Name, File Hash etc. from the logs.

Raw Log

```
Jan 1 20:28:02 knight sshd[20336]: Failed password for root from 218.49.183.17 port 49869 ssh2
```

↓ **Parsing**

Parsed Event

Metadata

Event = Failed Password

Username = root

Source IP = 218.49.183.17

Source Port = 49869

Protocol = ssh

What is Normalization?

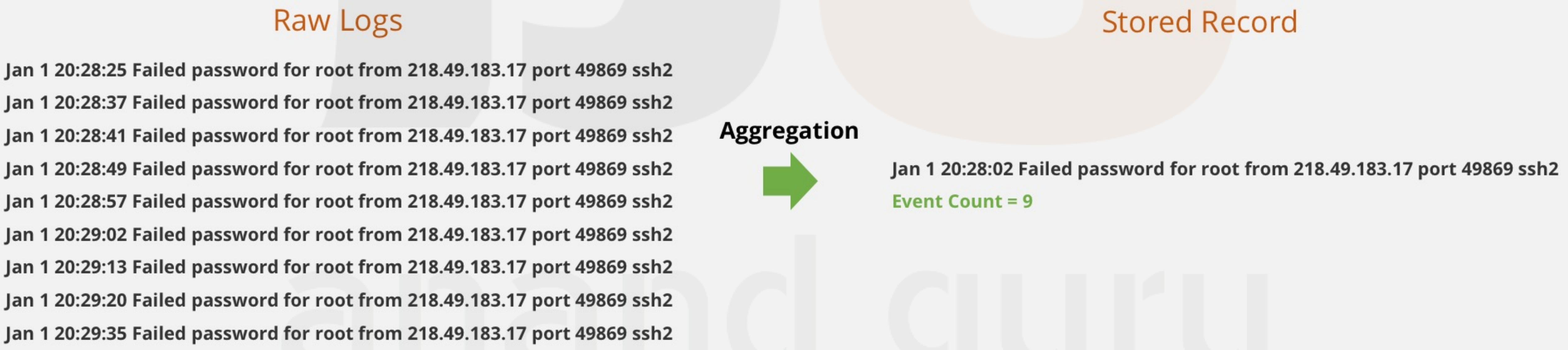
- Normalization is a process of bringing all events in to one common structure to deliver a homogeneous view
- It could be time normalization (bring events from various devices from different geo-location to a common time-zone)
- Identifying common event attributes (Like categorization – stamping all login, logout events as Authentication)

<u>Please Note:</u> For some SIEM tools **Normalization = Parsing**

What is Aggregation?

What is the use of aggregation?

- It is the process of merging similar logs that occur over a period of time.
- For example if there are 20 failed login events by a user on a server, the server would generate 20 logs. But, instead of storing all the 20 logs, SIEM will only store 1 record.
- Aggregation greatly helps in conserving the disk space and also increases the performance.



Raw Logs

```
Jan 1 20:28:25 Failed password for root from 218.49.183.17 port 49869 ssh2
Jan 1 20:28:37 Failed password for root from 218.49.183.17 port 49869 ssh2
Jan 1 20:28:41 Failed password for root from 218.49.183.17 port 49869 ssh2
Jan 1 20:28:49 Failed password for root from 218.49.183.17 port 49869 ssh2
Jan 1 20:28:57 Failed password for root from 218.49.183.17 port 49869 ssh2
Jan 1 20:29:02 Failed password for root from 218.49.183.17 port 49869 ssh2
Jan 1 20:29:13 Failed password for root from 218.49.183.17 port 49869 ssh2
Jan 1 20:29:20 Failed password for root from 218.49.183.17 port 49869 ssh2
Jan 1 20:29:35 Failed password for root from 218.49.183.17 port 49869 ssh2
```

Stored Record

```
Jan 1 20:28:02 Failed password for root from 218.49.183.17 port 49869 ssh2
Event Count = 9
```

What is Correlation?

- Correlation can be defined as set of conditions that indicates a suspicious activities.

Examples:

- User activity during non-business hours
- VPN logins from multiple locations
- Multiple malwares on the same host

What are the different collections methods available in SIEM solution?

How do you on-board Windows Event Logs?

What are the log sources you have on-boarded?

Collection Method	Used for	Example Log Sources
WMI (Windows Management Instrumentation)	Windows Event Logs	Application, System and Security Logs
Syslog	Network Devices and Security Solutions	Routers, Switches, Firewall, Proxy, WAF etc.
Flat File	Applications/Servers that write logs on to a flat file	
CIFS (Windows)		DNS, DHCP
NFS (Linux)		Apache Logs, Linux
Agent WinCollect – IBM QRadar SIEM Collector Agent – McAfee ESM Universal Forwards - Splunk	Various logs source including Windows Event Logs, Flat file logs etc.	Application, System and Security Logs, DNS, DHCP etc.
API	Cloud logs, Threat Feeds	AWS Cloudtrail logs
DB Collectors (JDBC/ODBC)	Databased Logs	MySQL Audit Logs, McAfee ePO, Oracle DB Audit Logs etc.

What are pull and push collection methods?

- A pull method of collecting logs means, the SIEM is actively involved in collecting the logs, usually by logging in to the log source. This is done at regular frequency.

  Example: WMI, Flat File, DB Collectors, API

- In push method, the logs are pushed by the log sources and SIEM just listens on the assigned port and IP.

  Example: Syslog, Agent

Pull and Push are sometimes referred to as **Active** and **Passive** Collection respectively

Syslog Collection Method.

1. Default port for Syslog?
   - Syslog – 514
   - TLS Syslog – 6514
2. Is Syslog TCP or UDP?
   - It has both TCP and UDP version

While purchasing a SIEM, how do you size it?

How will you decide the capacity of SIEM you need?

- SIEM sizing is done in 2 ways – Events Per Second (EPS) and Data Indexed per day
- There are few methods to do this:
  1. We can set up a POC (proof of Concept) and onboard few log sources of each type and measure the EPS. Later we can multiply by appropriate number of devices.

     Example: If we had 200 Windows log source and one windows log source during POC generated 10 EPS, we will need 200 x 10 = 2000 EPS
  2. Easier method would be to use the vendor provided spreadsheet calculator and feed in all the data like, no. of windows log source, number of DNS, no. of R&S, no. of firewalls etc. This will give an approximate EPS. To be on safer side we should keep a extra buffer of 20-30%
- In order to calculate the amount of data indexed most SIEM vendors typically take 1 event is roughly equal to 400 bytes for many log source and 1kb for Windows Event Logs

  If we have 300 log sources that generate 10 EPS each, then EPS = 3000 and the amount of data indexed will roughly be 3000 x 400 (bytes) = 1,200,000 bytes/second

  1,200,000 x 60 x 60 x 24 = 103,680,000,000 ~= 103 GB per day

How long should we retain logs in SIEM?

- The retention is usually defined by the regulatory compliance. Like, PCI defines that (raw) logs must be stored for one year with the last three months available in an easily accessible storage.
- Parsed events should be retained for 90 days.

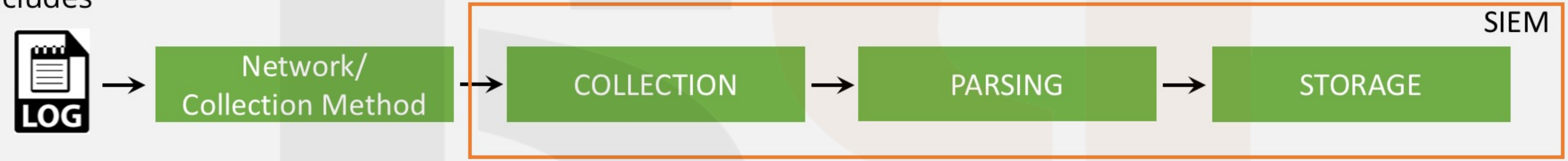
  Parsed events are typically used for analysis and reporting. It is very rare that we do analysis of events older than 90 days.
- Raw logs can be stored for an year.

How Frequently should you take SIEM backup?

- It is recommended to schedule the SIEM backup for every 7 days.
- But we should take manual backup every time we are making major changes or upgrades

How do you troubleshoot if any log source is not sending the logs?

- The non reporting logs sources are called as Silent Log Sources
- To troubleshoot a silent log source, we need to identify where the issue exists in the log flow. A typical log flow includes



- It could be at Log Source side - misconfiguration (wrong IP or port, necessary services not running, incorrect logging level etc.)
- The issue could be at network level - We can identify this by running packet capture on the collector (TCPDUMP for Linux based collectors and Wireshark for windows based) **`tcpdump –vvnni eth0 host <ip_logsource>`**
- The issue could be with collecting and parsing. We need to check appropriate services are running and check the logs files for any errors in SIEM
- Finally it could be a SIEM DB issue. which means the logs are being collected, parsed and stored, but UI is unable to query the DB. Usually a reboot would fix such issue.
- If none of this helps, I would bring in the vendor TAC

What is List/Watchlist/Reference Sets?

List is a collection of similar type of elements (like a list of IP addresses, list of all admin users). The lists can be used in filters and correlation rules.

Example:

1. List of all admin users
2. List of all Public IPs of a company
3. List of all Service Accounts

Lists are heavily used to integrate Threat Intelligence with SIEM

anand guru

SOC EXPERTS

Interview Questions on
Correlation Rules (Use Cases)

Anand Guru

Security+ | CySA+ | CEH | ECIH

Founder

SOC Experts

https://socexperts.com

What is Correlation?

Correlation is the process of identifying a suspicious activity by defining set of conditions.

Example: **A user account created during non-business hours**

Here there is a correlation between two (2) conditions.

- A event – User account created
- Time Condition – During non-business hours (Between 7pm and 7am)

How do you categorize correlation rules?

Different organization categorize correlation rules in different ways. Few of them are

Based on Device – Firewall based rules, AV based rules, Proxy based rules etc.

Based on Category – Malware, Access, Network, Database etc.

According to the phases of Cyber Kill Chain – Rule to detect Reconnaissance Phase or Exploit Phase etc.

What is a cross-platform correlation rule?

A correlation rule that involves at least two (2) different log source is called a cross-platform correlation rule.

Example 1: **High severity IPS alert for a Vulnerable host**

Here we are correlating an event from IPS plus we are using the data from the Vulnerability Assessment log source

Example 2: **Multiple RDPs after VPN access**

Here we are correlating events from Firewall (for VPN access) and any server based on an authentication event.

Malware Use cases.

Sl. No.	Use case	Description	Pre-requisites	Detection logic
1	**Malware detection on a Server**	If there is a malware detection on a server, it is definitely worth taking a look at irrespective of the AV action.	Create a List in SIEM of all the servers	Category=Malware Host (belongs to) Server List

2	**Unhandled Malware**	This is when the AV detects the malware but is unable to clean, delete or quarantine	None	Category = Malware
				Action = Delete failed OR Quarantine failed or Clean Failed

3	**Same Malware on Multiple Host**	Indicates several users are targeted via an email or a commonly used website	None	Category= Malware No. of Unique host = 5 Time Windows = 1 hour Malware Name is constant (group by)
4	**Multiple Malware Infection on a Host**	Indicates either the user is trying to download or copy a malicious file over and over again. OR a malware is partially executed and trying to perform a activity that is being detected as malicious by AV	None	Category = Malware No. of Event = 5 Time Window = 1 hours Host should be constant (group by)
5	**Outbound Communication to Blacklisted IP** OR **Possible Botnet Activity Detected**	A compromised host is initiating communication to its Command & Control	Create a List in SIEM of all Blacklisted IPs. This is done through Threat intelligence integration	Log Source = Firewall Direction = Local2Remote Destination IP (belong to) Blacklisted IP List
6	**Too Many DNS Lookup Failures**	Indicates the presence of Domain Generating Algorithm. DGAs are used by malware authors to avoid detections from Threat Intelligence.	None	Log Source = DNS DNS Response =NXDOMAIN No. of Event = 1000 Client is constant
7	**High Resource (CPU or Memory) Utilization**	High resource consumption is an indication of malware activity	Install an agent on the servers that will provide the resource utilization data	Avg. Memory Consumption for 10 minutes > 90% OR Avg. CPU Utilization for 10 minutes > 90%
8	**Unauthorized Process Detected**	A new (unknown) process is running in a server	Install Sysmon to collect process related information. Make a list of all authorized processes	Event = New Process Started Process Name (Doesn't belong to) Authorized Processes List

Use Cases on Firewall.

Sl. No.	Use case	Description	Pre-requisites	Detection logic
1	**Too many firewall Denies for same Source**	If an attacker is trying to connect over and over again and is being blocked. OR a malware is trying to connect to C&C and it is being denied	None	Event Type = Connection Denied No. of Events = 300 Time Window = 5 minutes With Source IP constant
2	**VPN logins from Multiple geolocations**	A user cannot connect to VPN from 2 geo-location	None	Event Type = VPN Authentication Unique Geolocations = 2 With Username held constant
3	**Horizontal Scan detected**	When a attacker tries to scan the available IPs as part of information gathering	None	Log Source = Firewall Unique Destination IPs = 10 Time Window = 1 minute With same Source IP
4	**Vertical Scan detected**	When a attacker tries to scan the available ports on a server as part of information gathering	None	Log Source = Firewall Unique Destination Ports = 100 Time Window = 1 minute With same Source IP and Destination IP
5	**Scanning on Remote Access Ports**	When an attacker tries to connect to company server on remote access ports	Create a List of all Remote Access ports like 3389, 22, 21, 1433, 3306 etc.	Log Source = Firewall Destination Port = List of Remote Access Ports No. of Event = 20 Time Window = 30 minute With same Destination IP
6	**High Volume of connection from country of concern**	Countries the company doesn't do business with or if the relationship of the country is not good with home country	List of all countries of concern	Log Source = Firewall Source Country = List of Countries of concern
8	**Outbound SMTP traffic from Unauthorized Host**	An infected machine might start sending spam email from inside the company.	List of all email servers	Log Source=Firewall Source IP != List of Email Server Destination Port = 25
9	**Proxy Bypass Attempt**	If any client or server tries to connect to internet directly (Usually done by users trying to do things that are not allowed. OR it could be a malware trying to connect to C&C	None	

Use Cases on AD and Windows Logs.

Sl. No.	Use case	Description	Pre-requisites	Detection logic
1	**Local account created**	User account created on server (not AD)	None	Event ID = 4720 Log Source != AD
2	**User added/removed to admin group**	Helps in monitoring accidental or attacker privilege escalations	Create a list of High Privileged Groups	Event ID = Group = List of High Privileged Groups
3	**Too many account lockouts**	Bruteforce is happening on several accounts	None	Event ID = 4740 No. of Events >10 Time Window = 1 hour
4	**Service Account Password Reset**	Service accounts are very sensitive as they have higher privileges and do not get locked out	List of all service accounts	Event ID = 4724 User in List fo Service Accounts
5	**AD Group Created/Deleted**	Groups are not created very often, so it is good to monitor group creations and deletions in AD	None	Event ID = 4731, 4727 for created Event ID = 4734, 4730 for deleted
6	**Domain Account Creation During Non-Business Hours**	Suspicious activity, Account created by Attacker	None	Event ID = 4720 Time (Not in) Monday – Friday 7am to 7pm
7	**Too many password resets**	Suspicious activity	None	Event ID = 4724 No. of Event > 10 Time window = 1 hour
8	**Audit Logs Cleared**	Attacker or a Admin is clearing the tracks	None	Event ID = 1102

Correlation Rules based on Cyber Kill Chain

Phase	Use case
Reconnaissance	• Horizontal Scan detected • Vertical Scan detected • Directory Traversal (alerted by WAF) • High Volume of connection from country of concern
Weaponization	• This phase cannot be detected as it is done by the attacker at his side.
Delivery	• Too many email from same domain • Too many email with same Subject line • Email with multiple attachments • Visit to malicious website
Exploit	• Too many file modifications • Registry changes detected
Install	• High Resource Utilization • New Process detected
Command & Control	• Communication to Bad reputation IP • Too many DNS Lookup failures
Actions on Objective	• File modification • High volume of data outbound • Critical Server Shutdown

How do you detect malware in the network without AV?

Behavior based malware detection.

- Outbound Communication to Blacklisted IP OR Possible Botnet Activity Detected
- Too Many DNS Lookup Failures (Indicates possible DGA running in the network)
- High Resource (CPU or Memory) Utilization
- Unauthorized Process Detected

How do you detect SQL Injection in SIEM?

We can write correlation to trigger on.

- SQLi related alert from IPS or WAF
- Unusual Username (User name with special characters used)
- Too many errors on Database
- Too many SELECT statements
- DROP command executed

These rules are typically run on **Database Audit Logs**

How do you detect Ransomware using SIEM?

We can write correlation to trigger on.

- Behavioral analysis for detecting user privilege escalation
- High Volume of administrator's logins.
- Monitoring of traffic parameters deviation from their baseline characteristics.
- Communication with malicious IP addresses, URLs, domains, and suspicious geographic destinations, as well as a traffic volume surge may indicate ransomware presence in a network.
- File Modifications (if we have File Integrity Monitoring events)

Correlation Rule to detect Phishing Email.

We can write correlation to trigger on.

- Too many email from same domain
- Too many email with same Subject line
- Email from Blacklisted IP
- Email with multiple attachments
- Email blocked due to phishing link (Email gateway events)
- Communication to Bad URL

anand guru

SOC EXPERTS

Interview Questions on
Threat Intelligence

Anand Guru

Security+ | CySA+ | CEH | ECIH

Founder

SOC Experts

https://socexperts.com

What is Threat Intelligence?

- Threat intelligence is knowledge that allows organization to prevent or mitigate cyberattacks esp. zero-day malwares or exploits.
- It is a subscription based services offered by many vendors.
- Technically TI is a database of Indicators of Compromise.

Name few open source Threat Intelligence feeds.

- Abuse.ch
- OSINT
- threatfeeds.io
- autoshun.org
- malwaredomainlist.com

Name few commercial Threat Intelligence feeds.

- IBM X-Force Exchange
- Anomali ThreatStream
- Palo Alto Networks AutoFocus
- FireEye iSIGHT Threat Intelligence
- Recorded Future

What is an IOC?

- IOC Stands for Indicators of Compromise. Its an attribute (forensic data) associated with an attack.
- IOC focuses on what of an attack.
- Attributes associated with an attack might include - **IP address, URL, email, file hash etc.**

What is IOA?

- IOA stands for Indicators of Attack.
- IOAs focus more on the WHY and intent of an actor.
- IOA is some events that could reveal an active attack before indicators of compromise become visible. Like, unknown process running
- Unlike Indicators of Compromise (IOCs) used by legacy endpoint detection solutions, indicators of attack (IOA) focus on detecting the intent of what an attacker is trying to accomplish.

What Are the Common Indicators of Compromise obtained from Threat Intelligence?

- **IP addresses, URLs and Domain names**: An example would be malware targeting an internal host that is communicating with a known threat actor.
- **Email addresses, email subject, links and attachments**: An example would be a phishing attempt that relies on an unsuspecting user clicking on a link or attachment and initiating a malicious command.
- **Registry keys, filenames and file hashes and DLLs**: An example would be an attack from an external host that has already been flagged for nefarious behavior or that is already infected.

What security solutions use Threat Intelligence?

- In todays world almost every prevention and detection system use TI feeds.
- AV solutions can use to check the malicious hashes
- Firewall can use TI to check blacklisted IP etc.

How does Threat Intelligence work?

Threat Intelligence Works in 2 ways

- Few TI feeds let you download the IOC database on-prem (like integrating into SIEM lists)
- Few other TI, works as a subscription based, every time you need to check the reputation of a file, URL or IP address, the security solution makes a quick light-weight query to the TI server, get the responses and take appropriate actions.

Where do you install Threat Intelligence in the network?

This is a trick question.

- TI is not installed on-prem, it is a subscription based services offered by many vendors.

Why Is Threat Intelligence Important?

- TI helps to keep companies informed of the advanced threats, exploits and zero-day threats that they are most vulnerable to and how to take action against them.

What is US-CERT?

- It is a website maintained by US Department of Homeland Security. It is a good source of TI.
- US-Cert release information about new threats in the form of Technical Alerts

Example of how you have consumed TI?

- Integrating TI feeds with SIEM
- Using IPVoid , URLVoid or VirusTotal during analysis of any alert
- Ad-hoc reports for latest attacks (using their IOCs)

How TI can be integrated with SIEM?

- TI can be integrated using Lists. These lists should be updated regularly to get the latest IOCs

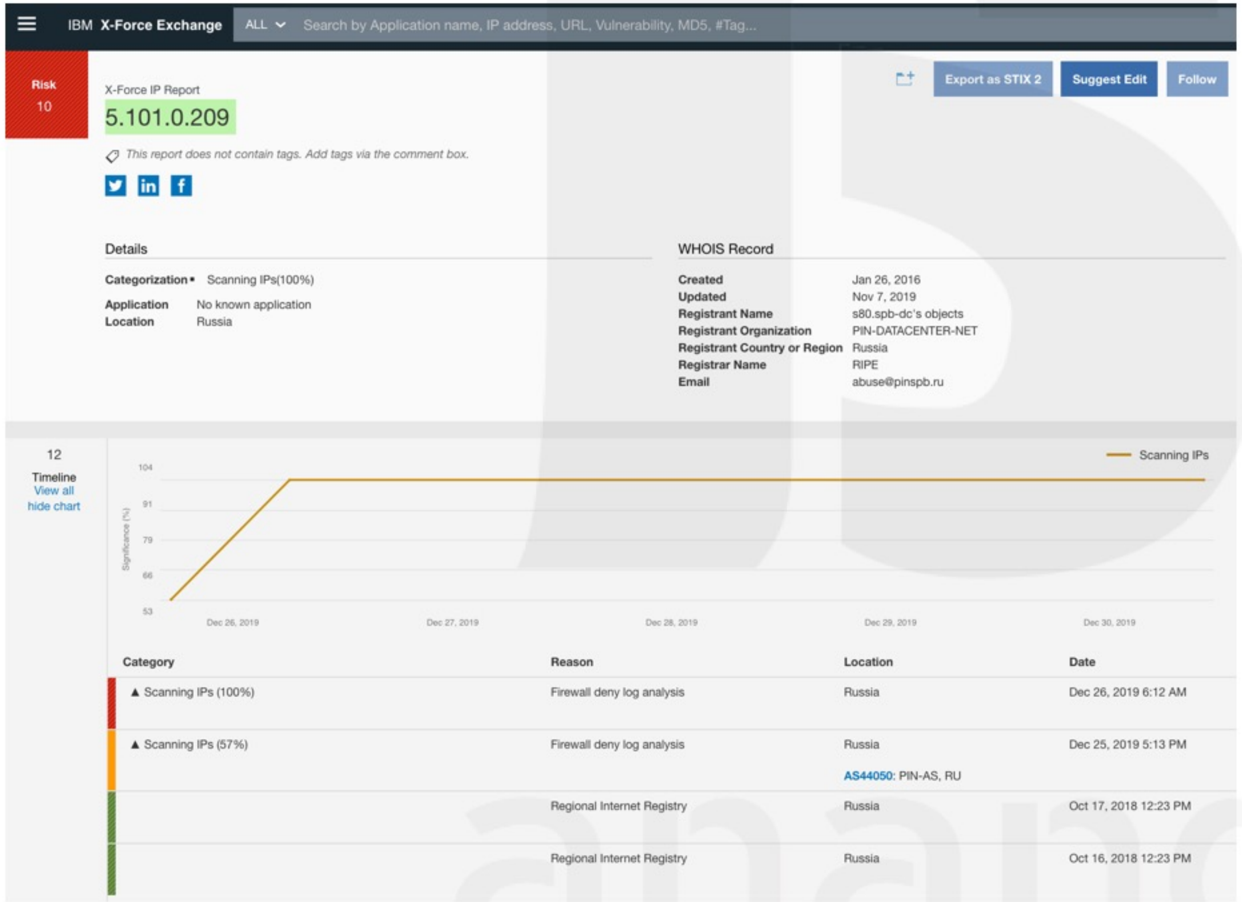
What are TAXII and STIX?

- Structured Threat Information Expression (STIX™) is a language and serialization format used to exchange cyber threat intelligence (CTI).
- Structured Threat Information eXpression (STIX) is a structured language for cyber threat intelligence
- Trusted Automated eXchange of Indicator Information (TAXII™) is a free and open transport mechanism that standardizes the automated exchange of cyber threat information.
- A transport mechanism for sharing cyber threat intelligence
- Example: http://hailataxii.com/

STIX states the what of threat intelligence, while TAXII defines how that information is relayed. STIX and TAXII are machine-readable and therefore easily automated.

Which is you favorite TI?

- IBM X-Force
  - Provides an exact score
  - Gives a timeline of how the IP was behaving over a period of time



IBM X-Force Exchange
ALL
Search by Application name, IP address, URL, Vulnerability, MD5, #Tag...
Export as STIX 2
Suggest Edit
Follow

Risk 10

X-Force IP Report

5.101.0.209

This report does not contain tags. Add tags via the comment box.

Details

Categorization •	Scanning IPs(100%)
Application	No known application
Location	Russia

WHOIS Record

Created	Jan 26, 2016
Updated	Nov 7, 2019
Registrant Name	s80.spb-dc's objects
Registrant Organization	PIN-DATACENTER-NET
Registrant Country or Region	Russia
Registrar Name	RIPE
Email	abuse@pinspb.ru

12

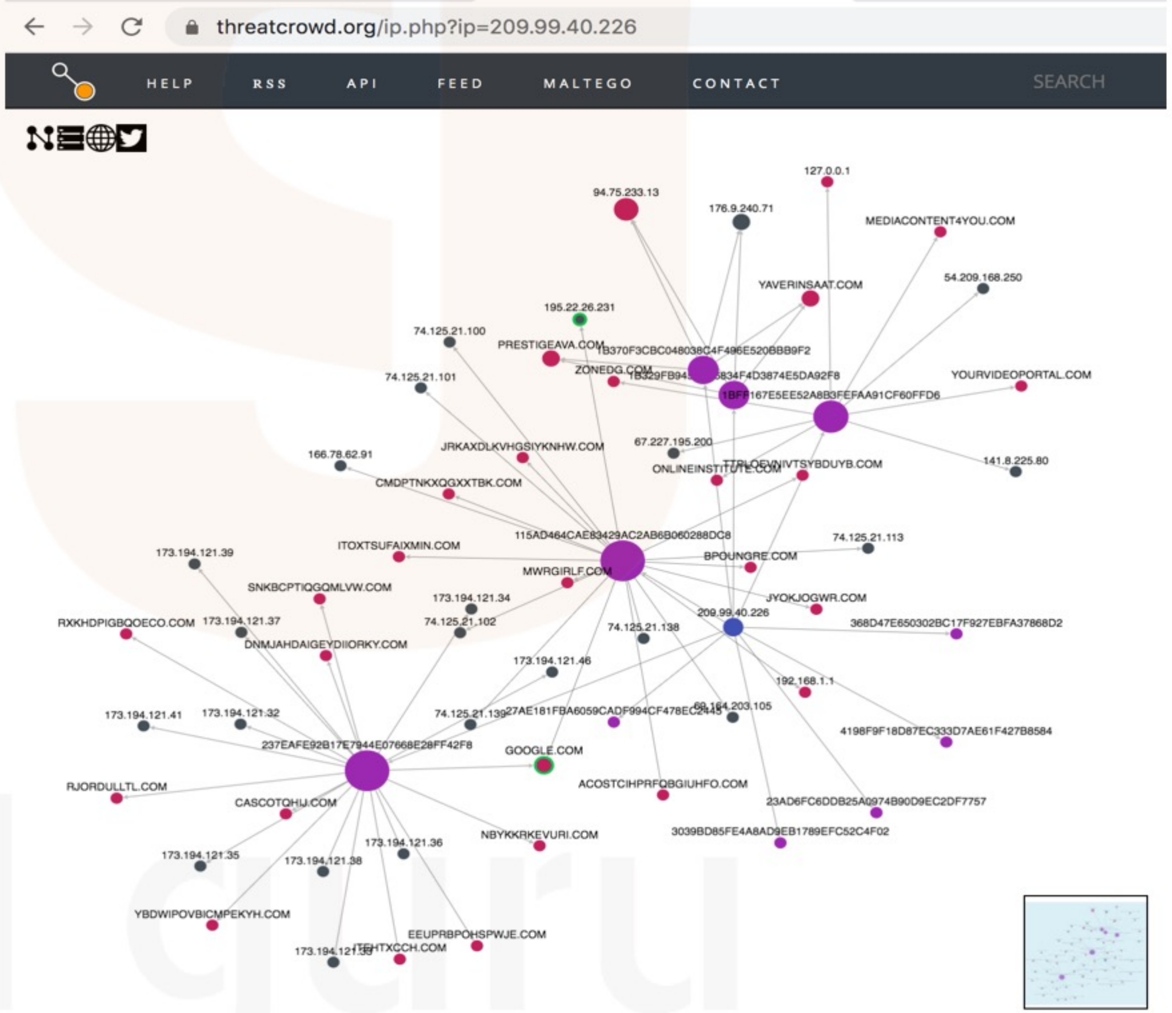
Timeline

View all

hide chart

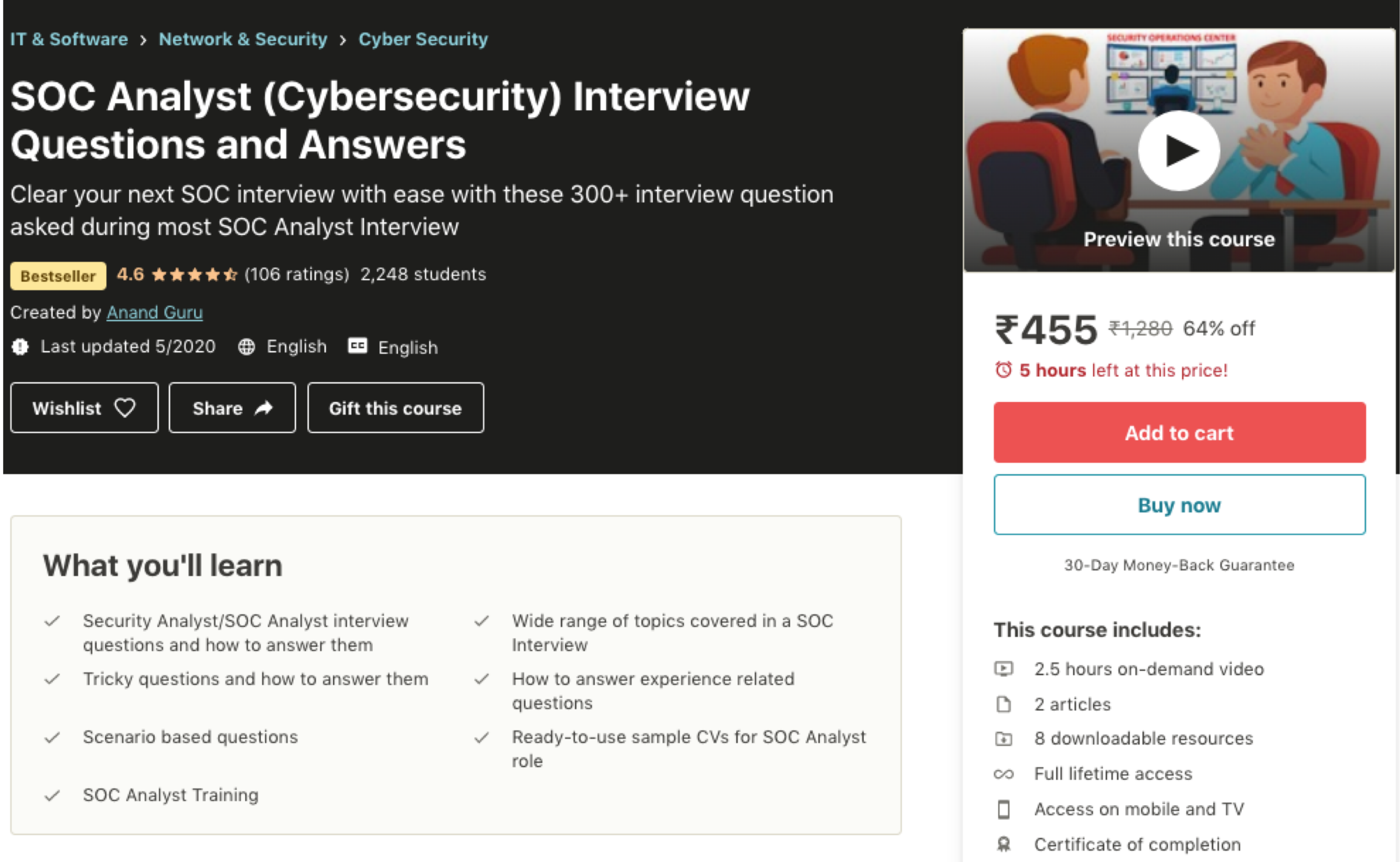
Category	Reason	Location	Date
▲ Scanning IPs (100%)	Firewall deny log analysis	Russia	Dec 26, 2019 6:12 AM
▲ Scanning IPs (57%)	Firewall deny log analysis	Russia AS44050: PIN-AS, RU	Dec 25, 2019 5:13 PM
	Regional Internet Registry	Russia	Oct 17, 2018 12:23 PM
	Regional Internet Registry	Russia	Oct 16, 2018 12:23 PM

- Threat Crowd
  - Gives a graphical representation of association of various attributes like domain name, IPs and file hashes



threatcrowd.org/ip.php?ip=209.99.40.226

Full course on Udemy



IT & Software › Network & Security › Cyber Security

SOC Analyst (Cybersecurity) Interview Questions and Answers

Clear your next SOC interview with ease with these 300+ interview question asked during most SOC Analyst Interview

Bestseller 4.6 ★★★★☆ (106 ratings) 2,248 students

Created by Anand Guru

Last updated 5/2020 English English

₹455 ~~₹1,280~~ 64% off

5 hours left at this price!

30-Day Money-Back Guarantee

What you'll learn

- ✓ Security Analyst/SOC Analyst interview questions and how to answer them
- ✓ Tricky questions and how to answer them
- ✓ Scenario based questions
- ✓ SOC Analyst Training
- ✓ Wide range of topics covered in a SOC Interview
- ✓ How to answer experience related questions
- ✓ Ready-to-use sample CVs for SOC Analyst role

This course includes:

- 2.5 hours on-demand video
- 2 articles
- 8 downloadable resources
- Full lifetime access
- Access on mobile and TV
- Certificate of completion

Interview Questions on

Analysis & Incident Response

Anand Guru

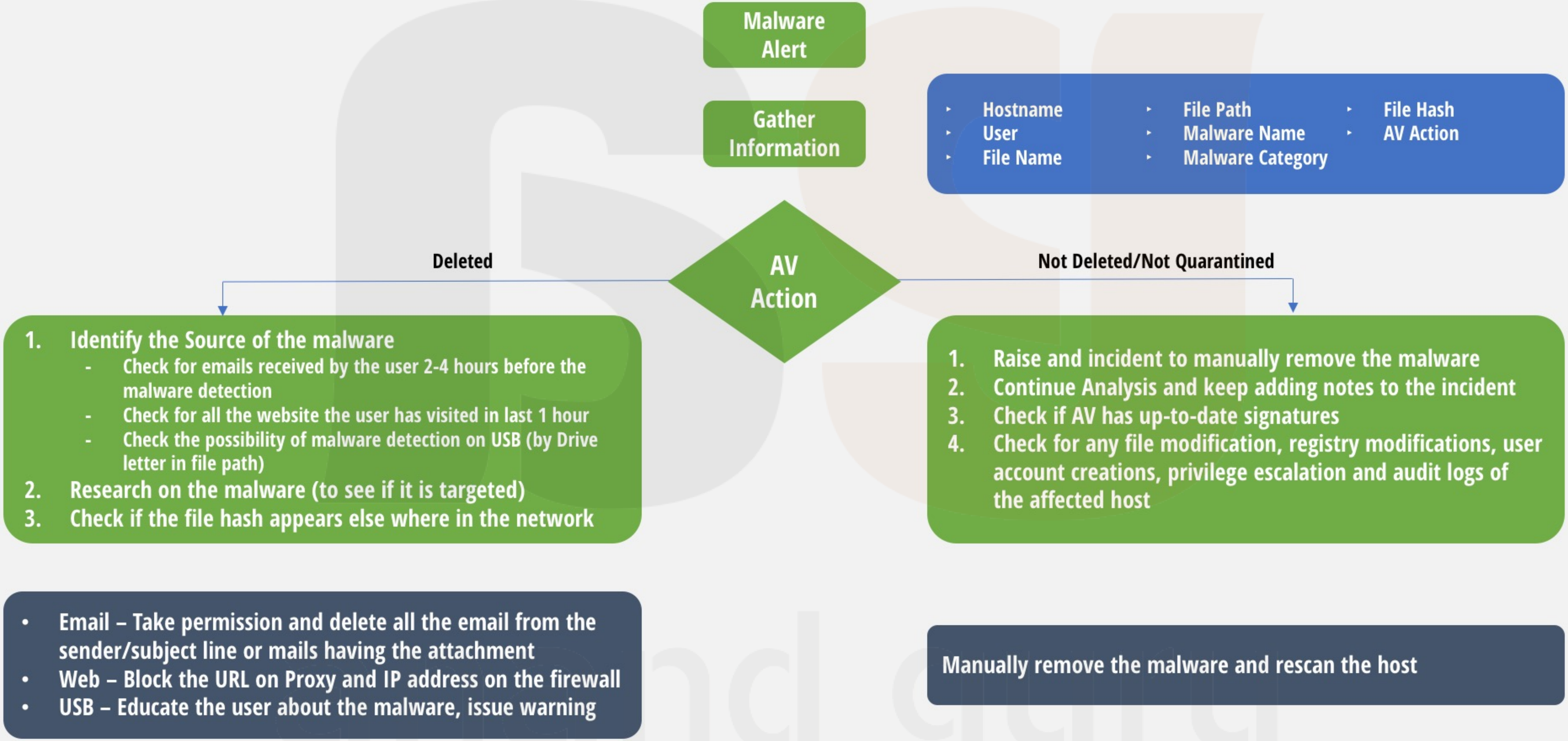
Security+ | CySA | CEH | ECIH

Founder

SOC Experts

https://socexperts.com

How do you handle a malware alert?



Malware Alert

Gather Information

- Hostname
- User
- File Name
- File Path
- Malware Name
- Malware Category
- File Hash
- AV Action

AV Action

Deleted

1. Identify the Source of the malware
   - Check for emails received by the user 2-4 hours before the malware detection
   - Check for all the website the user has visited in last 1 hour
   - Check the possibility of malware detection on USB (by Drive letter in file path)
2. Research on the malware (to see if it is targeted)
3. Check if the file hash appears else where in the network

- Email – Take permission and delete all the email from the sender/subject line or mails having the attachment
- Web – Block the URL on Proxy and IP address on the firewall
- USB – Educate the user about the malware, issue warning

Not Deleted/Not Quarantined

1. Raise and incident to manually remove the malware
2. Continue Analysis and keep adding notes to the incident
3. Check if AV has up-to-date signatures
4. Check for any file modification, registry modifications, user account creations, privilege escalation and audit logs of the affected host

Manually remove the malware and rescan the host

How do you remove a malware manually?

Step 1: Download Process Explorer and enable VirusTotal integration

Step 2: Run Process Explorer and look for the malicious process

Step 3: Identify the path of the process

We cannot delete the file from the path as it is currently running. If we try killing the process it comes up again immediately.

Step 4: Boot the machine in safe mode

In safe mode only minimum required windows process will run, there by preventing the malware from running.

Step 5: Delete the malicious file from the identified path

Step 6: Boot in standard mode and run a full scan

Should the machine be removed from the network?

Depends on the host in question, if it is a critical server and there are no redundant servers, we cannot isolate it from the network

How do you work on a Phishing Alert?

Phishing Mail Reported

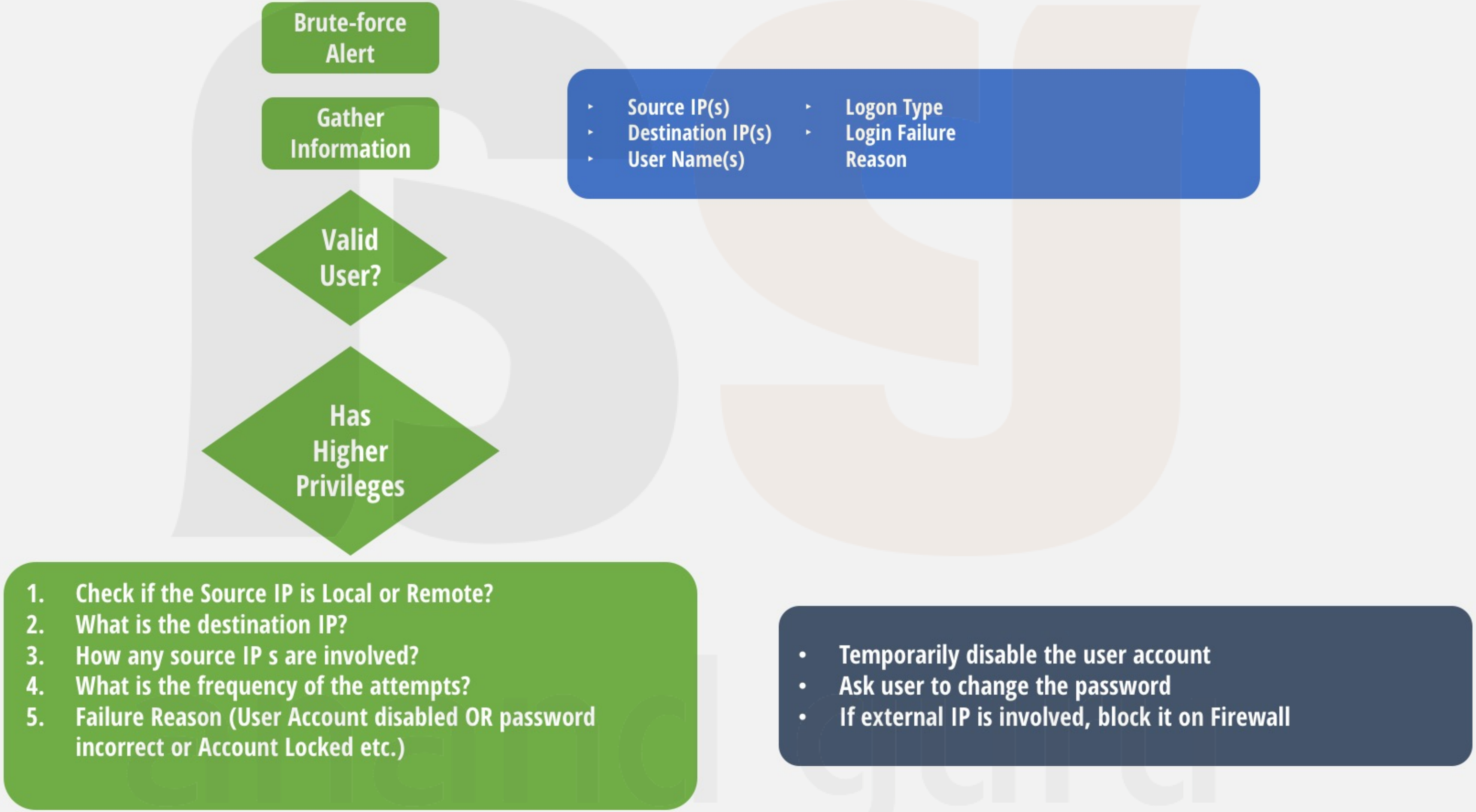
Open the Mail in .MSG format

1. Is the mail from public domain (like gmail, yahoo etc.)?
2. Is the domain name misspelled (like amazone.com)?
3. Is the email poorly written (grammar mistakes, incorrect use of words etc.)? Attackers do this to bypass standard filtering.
4. Does the email create a sense of urgency?
5. Right click on link and 'Copy link Address' and paste the URL on a notepad.
6. Copy the Internet Header
7. Copy the email to a sandbox and download attachments

1. Submit the URL to www.urlvoid.com and check the reputation.
2. Check the domain in WHOIS lookup to identify the IP address of the domain. Check the reputation of the IP at www.ipvoid.com
3. Paste the Internet Header to www.mxtoolbox.com (Analyze Headers)
    - Check for DMARC compliance
    - Check for SPF Alignment and Authentication
    - Check the DKIM Alignment and Authentication
4. Check the Return-Path
5. Check the reputation of IP address and domain names that appear in the header information

- Block the domain at the Email Gateway
- Block associated IPs at Firewall
- If there are other copies of email in other users mailbox, take permission to delete them
- Educate the user of the techniques used in the phishing email

How do you investigate a Brute-force Attack?



Brute-force Alert

Gather Information

- Source IP(s)
- Destination IP(s)
- User Name(s)
- Logon Type
- Login Failure Reason

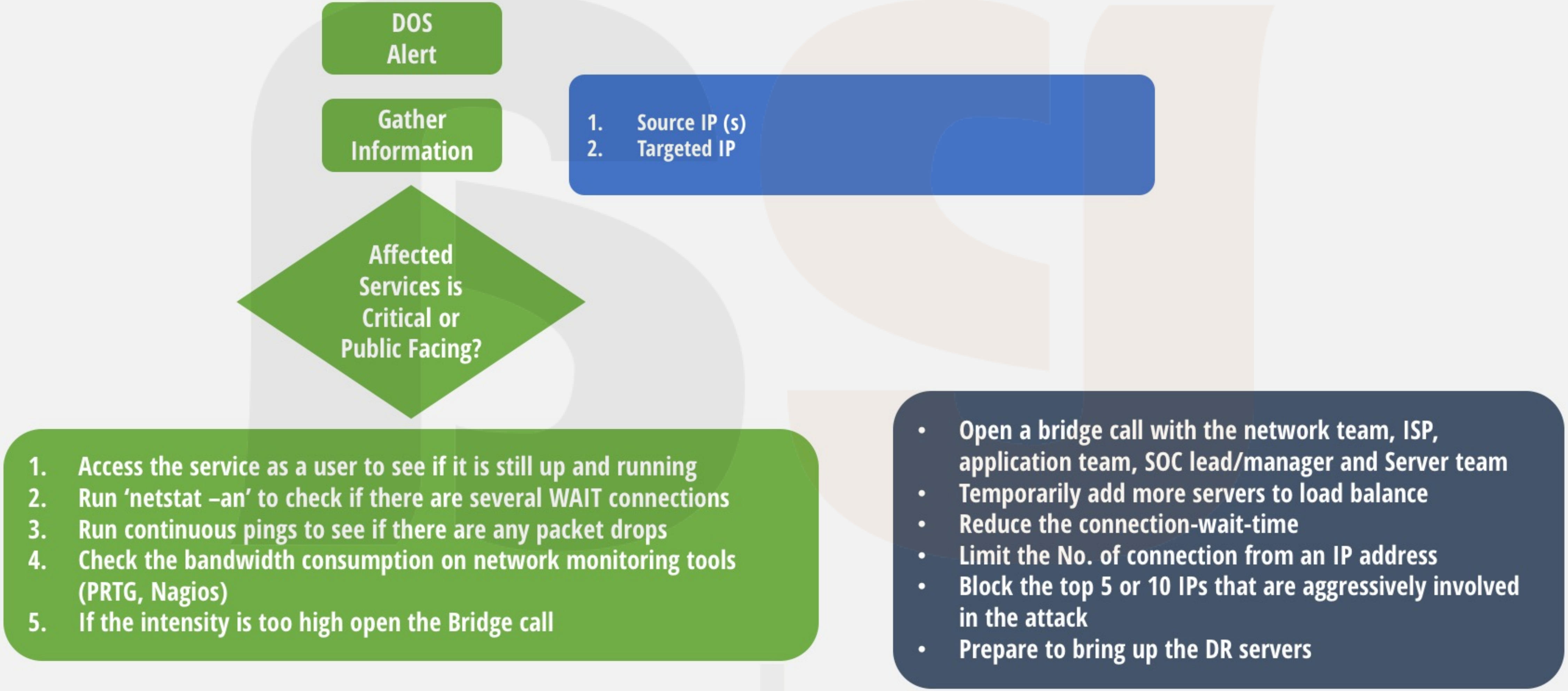
Valid User?

Has Higher Privileges

1. Check if the Source IP is Local or Remote?
2. What is the destination IP?
3. How any source IP s are involved?
4. What is the frequency of the attempts?
5. Failure Reason (User Account disabled OR password incorrect or Account Locked etc.)

- Temporarily disable the user account
- Ask user to change the password
- If external IP is involved, block it on Firewall

How do you analyze a DOS attack?



DOS Alert

Gather Information

1. Source IP (s)
2. Targeted IP

Affected Services is Critical or Public Facing?

1. Access the service as a user to see if it is still up and running
2. Run ‘netstat –an’ to check if there are several WAIT connections
3. Run continuous pings to see if there are any packet drops
4. Check the bandwidth consumption on network monitoring tools (PRTG, Nagios)
5. If the intensity is too high open the Bridge call

- Open a bridge call with the network team, ISP, application team, SOC lead/manager and Server team
- Temporarily add more servers to load balance
- Reduce the connection-wait-time
- Limit the No. of connection from an IP address
- Block the top 5 or 10 IPs that are aggressively involved in the attack
- Prepare to bring up the DR servers

How to work on a Ransomware alert?

Ransomware Alert

Logic of the correlation rule will be based on some IOC of a Ransomware, so it is important to verify if the IOCs are reliable

Gather Information

1. Source IP (s)
2. IOCs (URL or Hash or IP address

1. Verify the credibility of the IOC. Use IBM Xforce or www.URLVoid.com to check the reputation and confidence level.
2. Gather information like IP address, track the host name (by DHCP logs).
3. Call the user and inform about the situation
4. Take remote and ensure the AV is running and has latest signatures.
5. Also, look for any indication of a ransomware attack (file extension, inaccessible files etc.)
6. If the alert is genuine, ask the user to disconnect from the network open a ticket and assign it to endpoint security team
7. Continue analysis to understand the source of the malware.
8. Look for any other infected machine with the help of IOC or source of malware.

- Identify the type of ransomware and the stage of encryption.
- If it is in the early stage of encryption, try to identify the process and kill it.
- DO NOT reboot the machine as it might render the machine useless
- If file are already encrypted try to look for decryption keys from reliable source (AV vendors)
- If it is a user machine, format it.
- If it is a server, format it and restore form the backup

Explain the analysis for a SQL Injection Attack

SQL Injection Attack Alert

Usually IPS and WAF can report SQL Injection attempts

Gather Information

1. Source IP (s)
2. Log Source (IPS/WAF)
3. Severity

1. Check the reputation of the IP address
2. Check if this IP address was involved in any recon activity on our servers
3. Look for suspicious events on the database (like configuration changes, strange queries, DROP statements etc.)
4. Check to see if there is any anomaly in SELECT statements.

- Raise a ticket to block the IP on the firewall.
- Raise a ticket to expedite the Patching process on the target server.

Walk through the steps you follow to analyze 'Communication to Bad Reputation IP' alert.

Possible Botnet Activity Alert

Gather Information

1. Source IP
2. Destination IP
3. Destination Port
4. Log Source
5. Device (Firewall/IPS/Proxy) Action

1. Check the reputation of the public IP. Check its history and what kind of malicious activity (scanning, C&C, spam etc.) it is involved in.
2. Check the destination port. If it is other than 80 and 443 and is allowed by Firewall → Raise a ticket and assign it to firewall team to block the traffic.
3. Check if the source host has latest AV signatures.
4. Identify the process involved in generating the traffic on the machine (use the tool TCPLogView)
5. Check if the IP address is associated with any domain name or malware distribution (www.virustotal.com or www.threatcrowd.org)
6. Get the associated file hashes and check if they ever appeared in your network.
7. Take the associated URL/Domain name and see if they were visited by any users.

- If the traffic is allowed, block the IP at Firewall level
- If it is done by a malware (botnet) remove it manually and run a full scan on the machine.
- Ensure all the configurations on the affected system are intact
- Ensure the associated URLs are blocked
- Feed the associated file hashes to SIEM to detect and other attacks

‘IPS alert on a Vulnerable Host’ rule is triggered, how do you analyze it?

IPS alert on a Vulnerable Host Alert

Gather Information

1. Source IP
2. Destination IP
3. Destination Port
4. IPS Alert Name/Severity

1. Check the reputation of the source IP.
2. Check the IPS Alert and understand what it means and the severity of the alert.
3. See if there is an associated vulnerability (exploit signature of IPS) to the alert.
4. Research on the vulnerability using the CVE number. Look for affected OS, application and their versions.
5. Check if the target server is using the vulnerable version.

- Raise a ticket to block the IP on the firewall.
- Raise a ticket to expedite the Patching process on the target server.

Steps you take to analyze 'Unknown Process Detected' alert.

Unknown Process Detected Alert

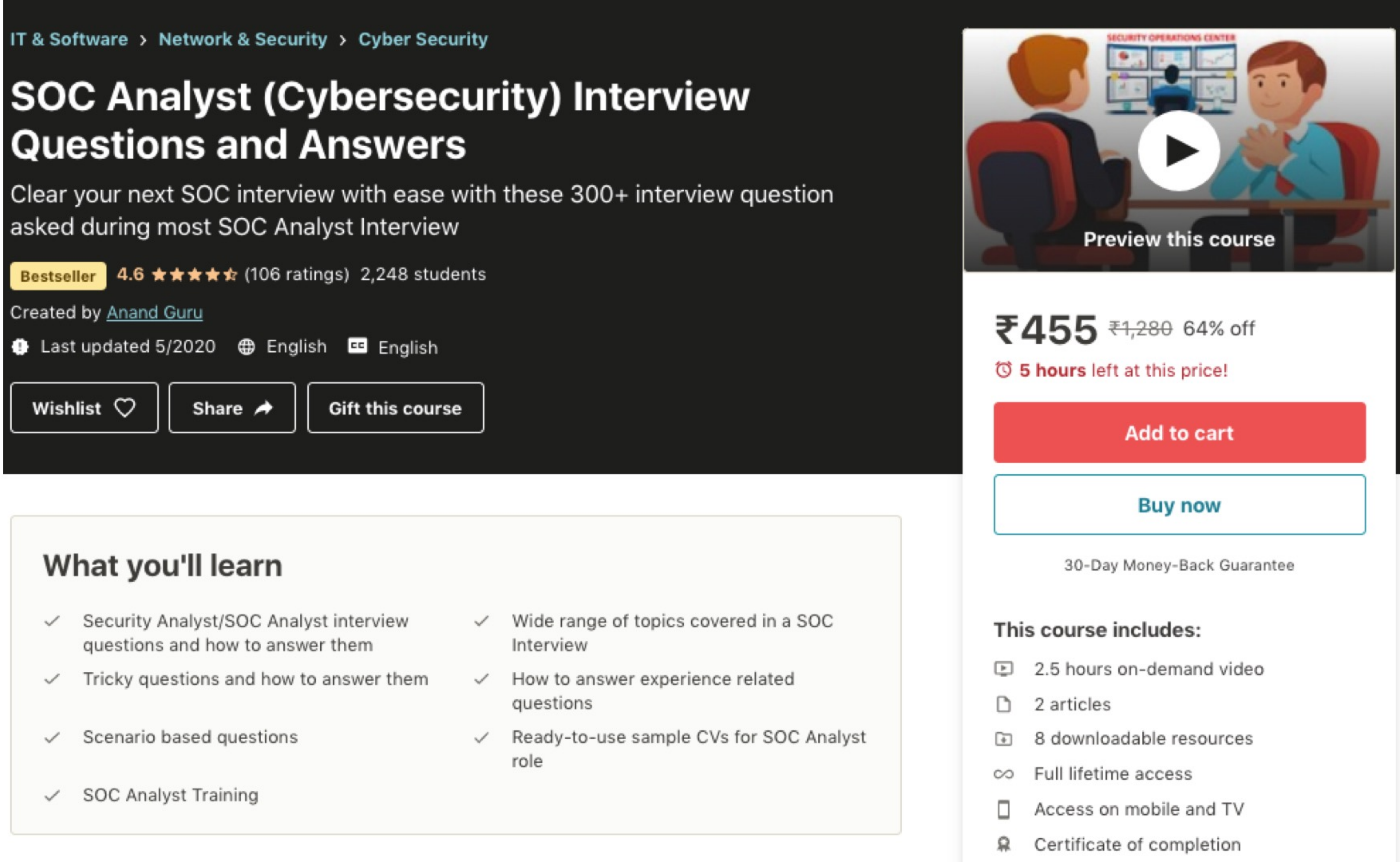
Gather Information

1. Source IP
2. Host
3. Process Name
4. Process Hash
5. Process path

1. Verify if it is a known malicious process by submitting the Hash to www.virustotal.com
2. If it is not a malicious process check with the user if he has installed any new software/application and ask for business justification
3. If the user is not aware of the running process, the new process has be analyzed (malware analysis) to check if it is malicious

- Raise a ticket to block the IP on the firewall.
- Raise a ticket to expedite the Patching process on the target server.

Full course on Udemy



IT & Software › Network & Security › Cyber Security

SOC Analyst (Cybersecurity) Interview Questions and Answers

Clear your next SOC interview with ease with these 300+ interview question asked during most SOC Analyst Interview

Bestseller 4.6 ★★★★☆ (106 ratings) 2,248 students

Created by Anand Guru

Last updated 5/2020 English English

₹455 ~~₹1,280~~ 64% off

5 hours left at this price!

30-Day Money-Back Guarantee

What you'll learn

- ✓ Security Analyst/SOC Analyst interview questions and how to answer them
- ✓ Tricky questions and how to answer them
- ✓ Scenario based questions
- ✓ SOC Analyst Training
- ✓ Wide range of topics covered in a SOC Interview
- ✓ How to answer experience related questions
- ✓ Ready-to-use sample CVs for SOC Analyst role

This course includes:

- 2.5 hours on-demand video
- 2 articles
- 8 downloadable resources
- Full lifetime access
- Access on mobile and TV
- Certificate of completion

anand guru

SOC EXPERTS

Interview Questions on
Vulnerability Management

Anand Guru

Security+ | CySA | CEH | ECIH

Founder

SOC Experts

https://socexperts.com

What is Vulnerability?

- A vulnerability is a weakness in a system, network or application.
  - System – Running with older version of a software
  - Network – Use of unsecure protocols
  - Application – No user input validation (leads to injection attacks)

What is Threat?

- Anything/Anyone that can exploit a vulnerability, intentionally or accidentally is a Threat

  Example: An attacker or Earthquake or Untrained Staff

What is Risk?

- The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability.

  Example: Financial losses because a e-commerce server is down, Loss of reputation etc.

What is Exploit?

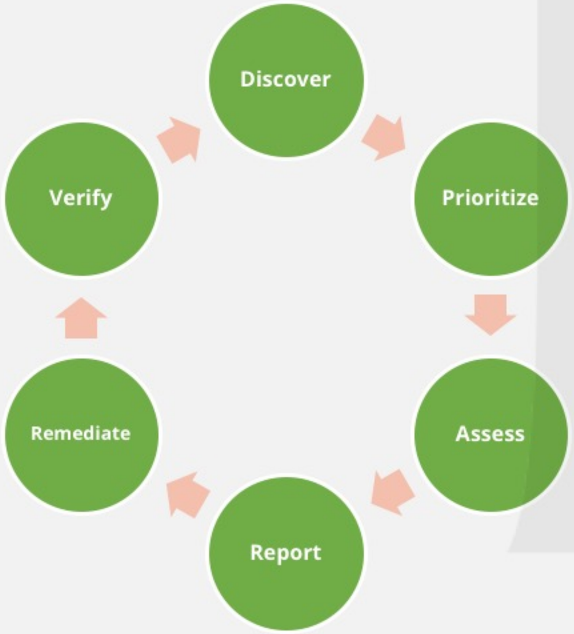
- A tool used to take advantage of the vulnerability.

  Example: Eternal Blue (take advantage of SMB vulnerability)

What is Vulnerability Assessment?

- Vulnerability Assessment is the process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems, applications and network infrastructures.
- Vulnerability Assessment team closely works with other infrastructure teams to help them remediate/patch vulnerabilities with the systems they manage.

Explain Vulnerability Management life cycle.



- **Discover** - Discover all the assets (using an host discovery scan)
- **Prioritize Assets** - Prioritize the assets based on the criticality and risk.
- **Assess** - Perform Vulnerability Assessment to identify vulnerabilities
- **Report** - Report all the vulnerabilities, based on criticality and business risk
- **Remediate** - Remediate the vulnerabilities by applying the patches or modifying the configurations
- **Verify** - Confirm that the patch has be applied successfully by rescanning the machines

What is the difference between VA and Penetration Testing?

- Vulnerability Assessment is all about identifying the vulnerabilities and reporting them for patching and remediation.
- Penetration Testing is going one step ahead (after identifying the vulnerabilities) and exploiting the vulnerability.
- Penetration Testing will help companies assess the risk in a better way.

Name few VA tools?

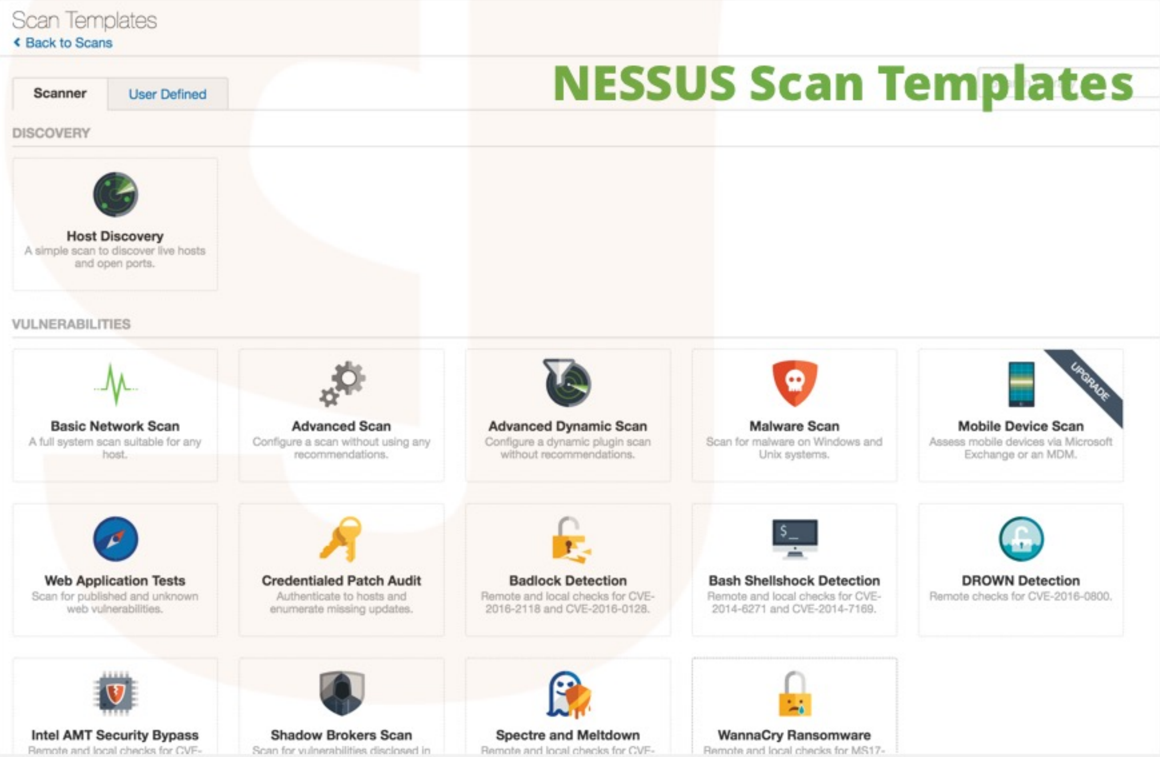
- The popular Vulnerability Assessment tools are
  - ✓ Tenable Nessus
  - ✓ Qualys Guard
  - ✓ Rapid7 Nexpose
  - ✓ OpenVAS (Open Vulnerability Scanner) – Open source tool

What is a Scan Template?

- A scan template is a pre-configured setting for a specific type of scan a user wants to perform.

Example:

- Advance Scan
- Host Discovery Scan
- PCI Compliance Scan
- Specific Vulnerability Scan (Scan for WannaCry Ransomware)



NESSUS Scan Templates

Scan Templates

‹ Back to Scans

Scanner | User Defined

DISCOVERY

Host Discovery
A simple scan to discover live hosts and open ports.

VULNERABILITIES

Basic Network Scan
A full system scan suitable for any host.

Advanced Scan
Configure a scan without using any recommendations.

Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.

Malware Scan
Scan for malware on Windows and Unix systems.

Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

UPGRADE

Web Application Tests
Scan for published and unknown web vulnerabilities.

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.

Bash Shellshock Detection
Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

DROWN Detection
Remote checks for CVE-2016-0800.

Intel AMT Security Bypass
Remote and local checks for CVE-

Shadow Brokers Scan
Scan for vulnerabilities disclosed in

Spectre and Meltdown
Remote and local checks for CVE-

WannaCry Ransomware
Remote and local checks for MS17-

How do VA Scanner identify Vulnerabilities?

- Most VA scanners use some kind of Scripting languages to scan the machines and the results are compared with the database of know vulnerabilities.
- A vulnerability scanner can also detect weak configurations and passwords, no password, default passwords.
- Some of the scripts looks for Registry values to identify the version and patch level of an application.

Where do you find Vulnerability details?

- Few good source of all the vulnerabilities are
  - www.cvedetails.com
  - www.nvd.nist.gov (National Vulnerability Database)
  - www.cve-mitre.org

What is CVE?

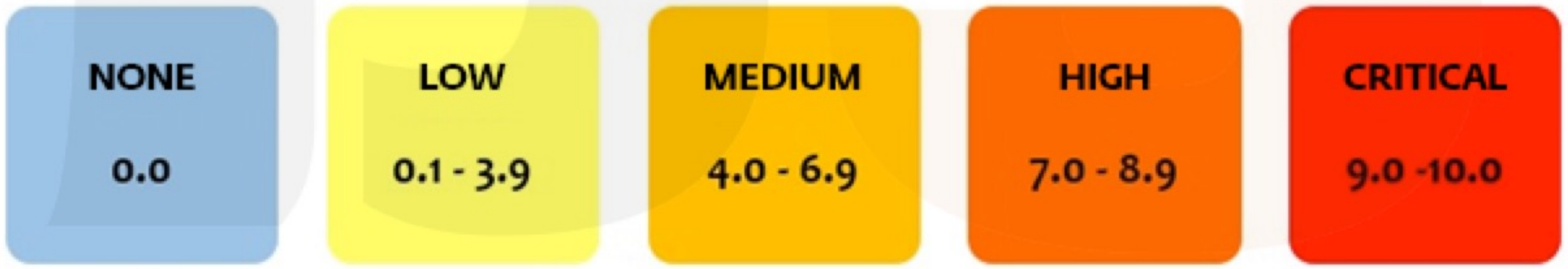
- CVE stands for Common Vulnerabilities and Exploits. It is a number given to each identified vulnerability.
- CVE is a list of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities.
- The format of the CVE is:

```
CVE prefix + Year + 4 Arbitrary Digits (CVE-YYYY-NNNN)
```

Example: `CVE-2019-1760`

What is CVSS?

- CVSS stands for Common Vulnerability Scoring System. It is an industry standard used by vendors to define the criticality of a vulnerability. The score ranges from 0 to 10.
- CVSS are categorized as below:



NONE	LOW	MEDIUM	HIGH	CRITICAL
0.0	0.1 - 3.9	4.0 - 6.9	7.0 - 8.9	9.0 -10.0

Categories of CVSS v3.0

How frequently should a Vulnerability scans be run?

When does a company run Vulnerability Scans?

- Vulnerability assessments are usually performed on a scheduled basis, typically Monthly once or Quarterly once.
- Also scan can be run on need basis. A solid example is when a new headline vulnerability emerges. When this vulnerability assessment is performed, the scan are configured to specifically look for the new vulnerability.

What is Patch Management?

- **Patch management** is the process of applying (installing) patches to a system or application in order to get new features, fix bugs or security issues.

Difference between Hotfix, Patch and Service Packs.

- **Hotfix** addresses only one bug(issue). Typically does not require a reboot.

  v8.5.0 to 8.5.0 Build 20200101

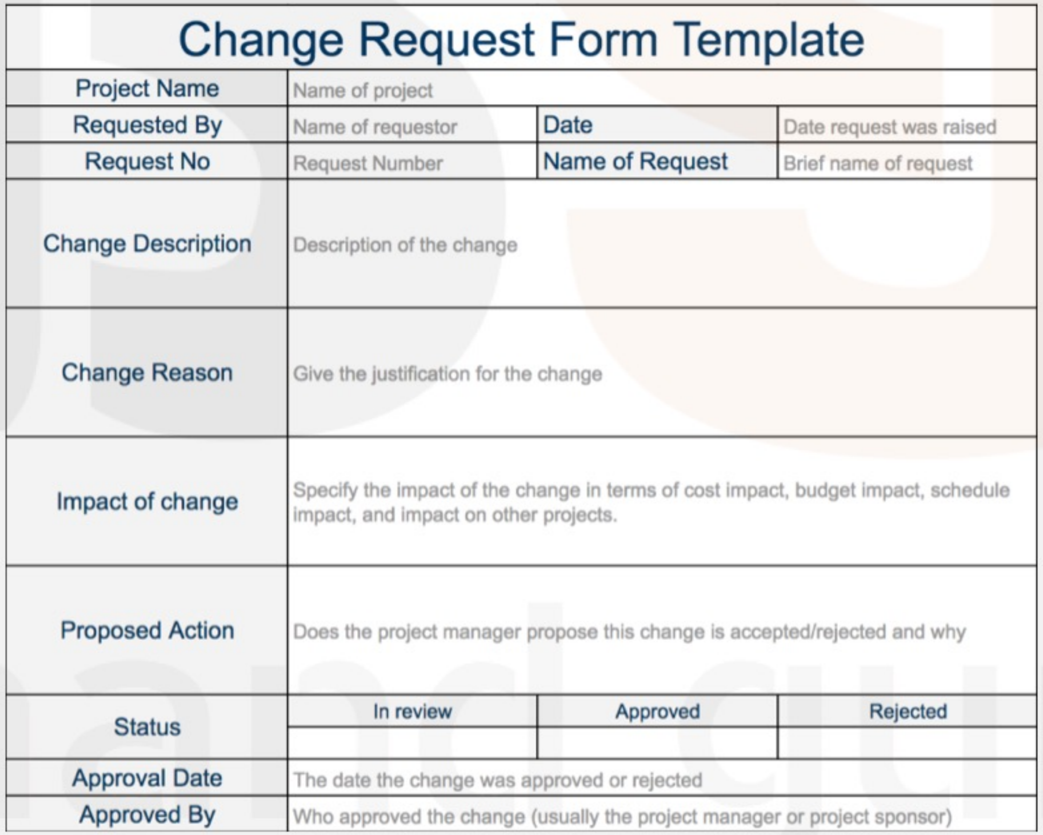
- **Patch** is a collection of hotfixes and new features. Usually requires a reboot of the system to be effectively applied.

  v8.5.0 to 8.5.1

- **Service Pack** is collection of patches.

What is Change Management?

- Change management is the process, tools and techniques to manage the people side of change to achieve the required business outcome.
- Change management helps in reducing the risk associated with the change.
- When a team (or individual) wants to perform a change in the server, they raise a Change Request (CR)



Change Request Form Template

Project Name	Name of project		
Requested By	Name of requestor	Date	Date request was raised
Request No	Request Number	Name of Request	Brief name of request
Change Description	Description of the change		
Change Reason	Give the justification for the change		
Impact of change	Specify the impact of the change in terms of cost impact, budget impact, schedule impact, and impact on other projects.		
Proposed Action	Does the project manager propose this change is accepted/rejected and why		
Status	In review	Approved	Rejected
Approval Date	The date the change was approved or rejected		
Approved By	Who approved the change (usually the project manager or project sponsor)		

What is Buffer Overflow Vulnerability?

- Buffer Overflow vulnerability is a weakness in an application that lets an attacker over-run the fixed length block of memory. It is possible that attacker might consume the entire memory there by slowing down or crashing the server. This leads to Denial of Service attack.

Example: CVE-2016-6808 - Buffer overflow in Apache Tomcat Connectors (mod_jk) before 1.2.42.

What is Remote Code Execution Vulnerability?

- Remote Code Evaluation is a vulnerability that when exploited gives the attacker execute commands on the compromised server.
- A Remote Code Evaluation can lead to a full compromise of the server.

Example: CVE-2019-1238 - VBScript Remote Code Execution Vulnerability

If a vulnerability cannot be patched immediately, what has to be done?

- Step up the security for the server
  - Like Tighten the configurations on OS, AV, Host Firewall etc.
- Check with IPS team if there is a signature available to detected if the vulnerability is being exploited, if so assign a high severity to it
- Increasing the level of monitoring on the server.
  - Typically done by putting the affected server(s) in a list and writing more sensitive rules.
  - Like if the default threshold for Brute-force is 100 attempts in 1 minute. On this server it will be 10 in 1 minute.

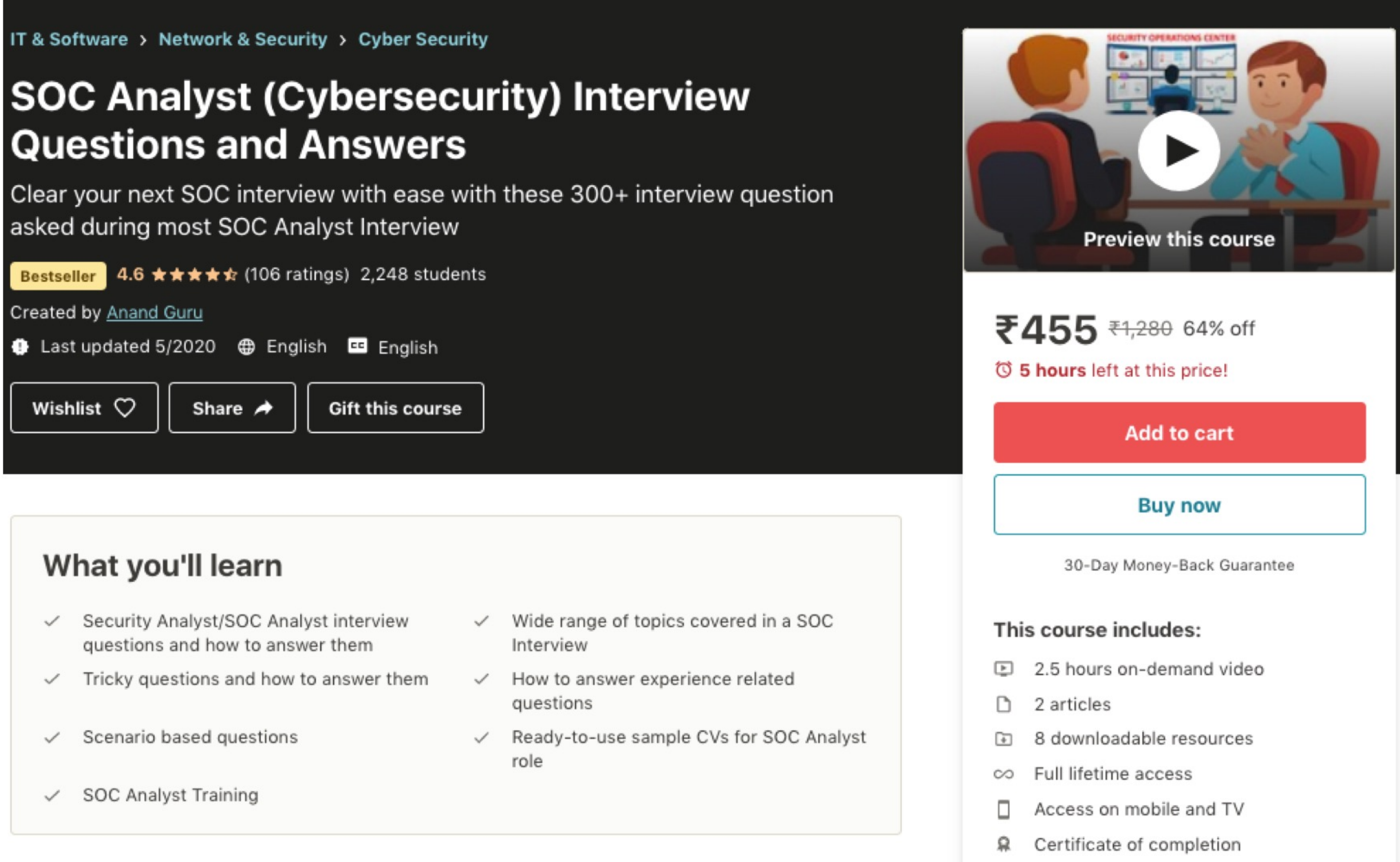
What are the vulnerabilities you have worked on?

- I can always recall working on the WannaCry Ransomware Threat.
- The weakness (vulnerability) was with Microsoft's SMBv1 **(MS17-010)**
- Microsoft had already released the patch.
- We had 800 Windows Servers and around 4000 Windows Client Machines.
- We were working closely with server/system team and vulnerability management team.
- Scans were scheduled almost hourly basis on different network segments.
- Pulling reports on a regular basis. We presented a report to our CISO every 3 hours once for almost 4 days. Till we got 98% of the machines patched.

What is the latest vulnerability you have heard of?

- Look at the latest vulnerability
- Get the Vendor, Product and Version of product it is present in.
- Try to remember the CVE number if possible.
- Understand how the vulnerability can be exploited.
- Check if a patch is already available.
- See if any major attacks have happened because of this vulnerability.
- Try to relate the vulnerability to your organization.
    - Did it affect the company you are working with?
    - How did you company handle the vulnerability?
    - What teams were involved in patching?

Full course on Udemy



IT & Software › Network & Security › Cyber Security
SECURITY OPERATIONS CENTER
Preview this course
Wishlist ♡
Share
Gift this course
Add to cart
Buy now

SOC Analyst (Cybersecurity) Interview Questions and Answers

Clear your next SOC interview with ease with these 300+ interview question asked during most SOC Analyst Interview

Bestseller 4.6 ★★★★☆ (106 ratings) 2,248 students

Created by Anand Guru

Last updated 5/2020 English English

₹455 ~~₹1,280~~ 64% off

5 hours left at this price!

30-Day Money-Back Guarantee

What you'll learn

- ✓ Security Analyst/SOC Analyst interview questions and how to answer them
- ✓ Tricky questions and how to answer them
- ✓ Scenario based questions
- ✓ SOC Analyst Training
- ✓ Wide range of topics covered in a SOC Interview
- ✓ How to answer experience related questions
- ✓ Ready-to-use sample CVs for SOC Analyst role

This course includes:

- 2.5 hours on-demand video
- 2 articles
- 8 downloadable resources
- Full lifetime access
- Access on mobile and TV
- Certificate of completion

anand guru

SOC EXPERTS

Interview Questions on **Threat Hunting**

Anand Guru

Security+ | CySA | CEH | ECIH

Founder

SOC Experts

https://socexperts.com

What is Threat Hunting?

Threat hunting is a human-driven, proactive and iterative approach which involves searching through networks & endpoints, to detect malicious activities that have evaded detection by existing automated tools.

Hunting is an offense-based approach that applies adversaries' tactics and techniques, and adopts their mindset when investigating signs of compromise within an organization.

Explain Threat Hunting Process.

The process involves 5 stages

1 - Hypothesis Generation: The aim of these hypotheses is to find evidence of threats before they are exploited, or even ones that are already being exploited.

2 – Validation of the hypotheses: Once a hypothesis has been defined, its validity needs to be verified. We then need to look for the existence of threats that fit this hypothesis. In this stage it is usual for some hypotheses to be discarded, while research into others is prioritized due to their likelihood or criticality.

3 – Finding evidence: From the results obtained in the previous search, we need to verify if a threat really exists. False positives and mistakes in configuration are set aside, and efforts are focused on the validated hypotheses.

4 – Discovery of new patterns: The attack is reconstructed to find any new patterns and tactics used to carry it out.

5 – Notification and enrichment: Using the knowledge generated during the Threat Hunting process, the automatic detection systems are enriched and improved. This way, the organization's global security is improved.

Why should we do Threat Hunting?

Advantages of threat hunting are as follows:

- Proactively Uncover Security Incidents
- Detect the undetected
- Improve the Speed of Threat Response
- Reduces False Positives and Improves SOC Efficiency
- Reduce dwell time. Hunting enables an organization to identify and stop adversaries early in the kill chain stops them from reaching their ultimate target.
- Evict adversaries with minimal business disruption.

Difference between Threat Hunting and Threat Detection?

Threat Detection is a reactive approach.

Use traditional preventive technologies and monitoring tools to detect a malicious activity.

Threat detection leads to mitigation.

Threat Hunting is a proactive approach.

Detect slow and stealth attacks that would otherwise go unnoticed by preventive technologies.

Threat hunting leads to threat detection and incident response.

What tools do you use for Threat Hunting.

Few of the threat hunting tools are

- **Sqrrl**
- **Vectra Cognito**
- **Exabeam Threat hunter**
- **Endgame**
- **DNIF**

Other tools that help during threat hunting include

- **EDR**
- **Threat Intelligence**
- **ELK for analytics**

Explain the different Threat Hunting Techniques.

Different thereat hunting techniques are as follows:

Searching: This is probably the most basic form of threat hunting. With this technique, you are trying to support your formulated hypothesis with information and data from a very specific set of defined search criteria

Clustering: This is more of a quantitative, statistically-based approach to threat hunting. With this technique, the threat hunter is attempting to “cluster” similar datasets from a larger pool of data, to find the hidden or unseen trends in these datasets

Grouping: In this scenario, the threat hunter is looking at different (or unique) artifacts that have been discovered and identifying them based on the same set of criteria that was used to formulate the original hypothesis

Stack Counting: This is another type of statistical technique. In this case, the threat hunter ascertains the total number of occurrences of a certain dataset by closely examining any sorts of outliers that may exist

Explain the OODA Strategy.

OODA is an abbreviation of Observe, Orient, Decide and Act. Military personnel apply OODA when they carry out combat operations. Likewise, threat hunters use OODA during cyberwarfare. In the context of threat hunting, OODA works as:

Observe: A first phase that involves routine data collection from endpoints

Orient: Understanding the collected data thoroughly and combining this information with other collected information to help understand its meaning.

Decide: Once you have analyzed the information, then you need to identify the course of action. If the incident occurs, threat hunters will execute the incident response strategy

Act: The last phase involves the execution of the plan to put an end to the intrusion and enhance the company's security posture. Further measures are taken to prevent the same type of attack in the future

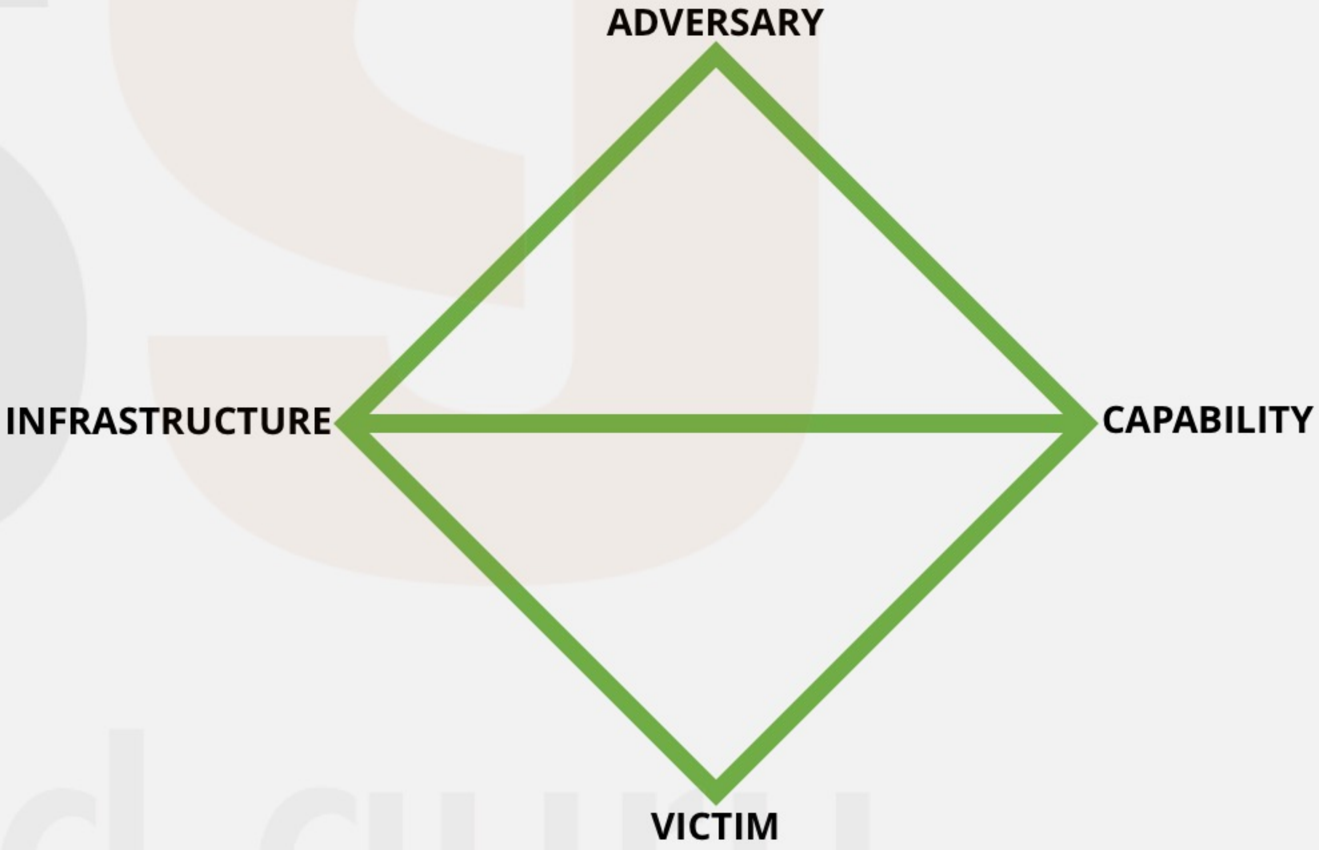
What is Diamond Model?

The Diamond Model emphasis the relationship between basic elements of any malicious activity.

It has 4 elements

1. **The Adversary**
2. **The Victim**
3. **Infrastructure**
4. **Capability**.

All malicious activity contains these elements.



What is MITRE ATT&CK? How is it used in Threat Hunting?

ATT&CK stands for Adversarial Tactics, Techniques and Common Knowledge.

It is a knowledge base of the attacks, the tactics and techniques used and associated APT groups.

It helps in mapping out an attack in various stages (called Tactics) and methods/tools (called Techniques) used at various stages.

MITRE ATT&CK framework is used by threat hunters

- To map various attack vectors.
- Identify the ones that your organization is susceptible to.
- Build hypothesis around the prioritized techniques.
- Hunt for the adversaries.

Give example of Threat Hunting Hypothesis.

1. Recognizing suspicious software

- This is useful in detecting malwares.
- Look for Event ID **4688**. Also use **sysmon** to enable logging of all process start and termination.
- Make a list of all standard processes that run in the network.
- Use process Hashes (some malwares can run with legit process names (like notepad.exe)

2. Detecting Command and Control Communication

- Malware communicate back to C2 servers for exfiltration data or get further instructions for the attack.
- They typically use common port number to avoid detection. But we can check for various combination of communication channels like:
  - Common Port & Common Protocol
  - Common Port & Uncommon Protocol
  - Uncommon Port & Common Protocol
  - Uncommon Port & Uncommon Protocol
- Hypothesis: Attackers may be operating on a C2 channel that uses a common protocol on a common network port
  - Look for unique artifacts pertinent to the protocol you are interested in. For example, if you are interested in identifying C2 in HTTP traffic, then you might consider looking for anomalous domains/URLs/User-Agent strings.
- Dataset to use:
  - HIPS logs
  - Firewall Logs
  - Proxy Logs
  - DNS Logs

Example of Threat Hunting Hypothesis.

3. Hunting for Internal Reconnaissance

Hypothesis: An attacker conducting internal reconnaissance would attempt to carry out host enumeration and automate these commands with a script

Look for these commands to be spawned by a script:

- whoami
- net user
- useraccount (WMIC)
- Get-NetIPConfiguration (PowerShell)
- hostname
- ipconfig
- nicconfig (WMIC)

Dataset to use:

- Process Names
- Process Hashes

What makes a person good at Threat Hunting?

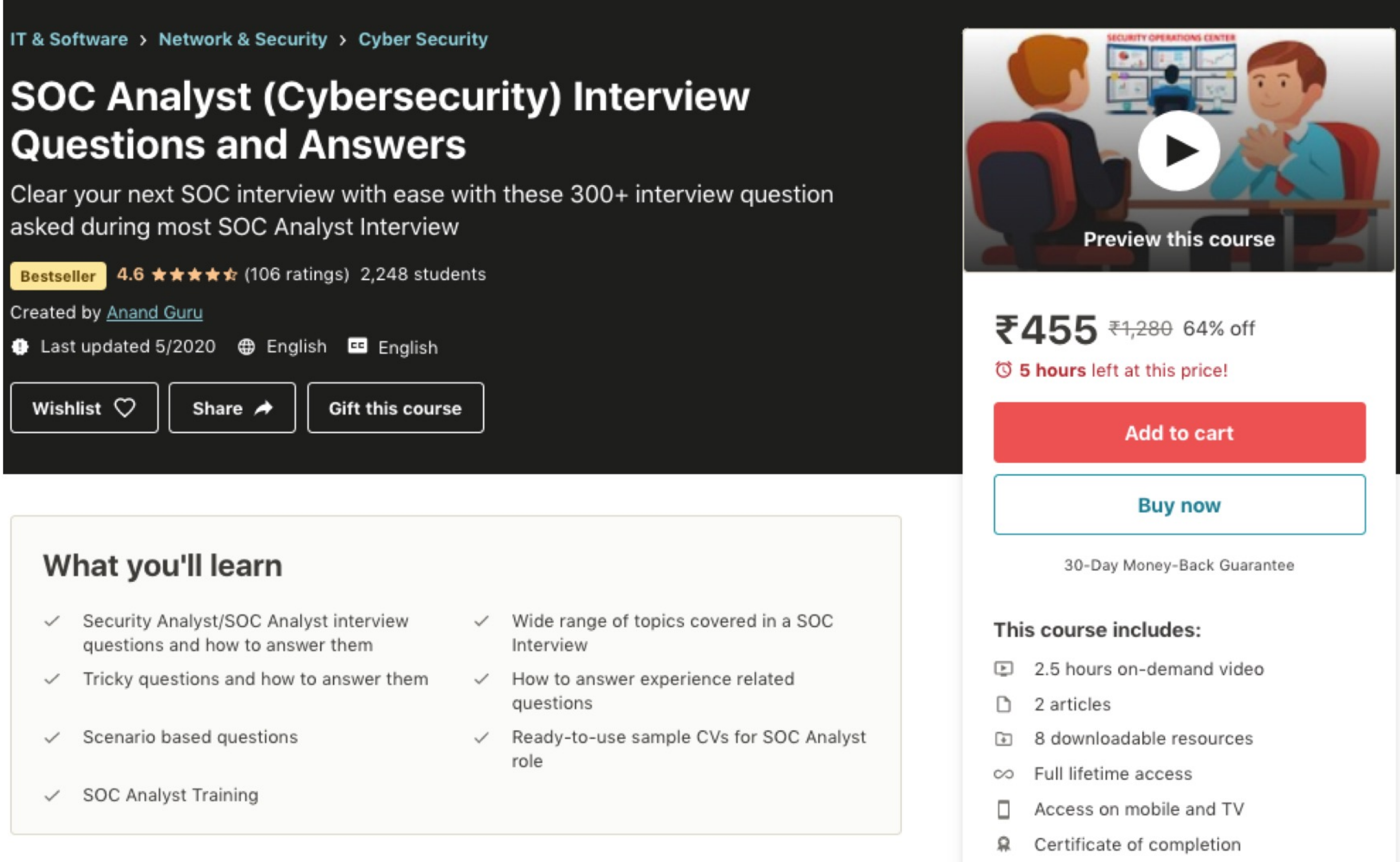
- Good understanding of various attack vectors (TTPs in ATT&CK framework)
- Hypothetical thinking: the ability to hypothesize threat attacks, source vectors, and organizational impact
- Good knowledge of organization infrastructure
- Good at pattern recognition
- Being aware of latest attack techniques
- Data Analytics
- Basic scripting knowledge for automation

How do you measure effectiveness of Threat Hunting?

Few of the key metrics in measuring effectiveness of threat hunting include:

- Number of incidents by severity
- False positive rate of transitioned hunts
- Dwell time of any incidents discovered
- Number of detection gaps identified and fixed
- Logging gaps identified and corrected
- Insecure practices identified and corrected
- Number of hunts transitioned to new analytics
- Any new visibility gained

Full course on Udemy



IT & Software › Network & Security › Cyber Security

SOC Analyst (Cybersecurity) Interview Questions and Answers

Clear your next SOC interview with ease with these 300+ interview question asked during most SOC Analyst Interview

Bestseller 4.6 ★★★★☆ (106 ratings) 2,248 students

Created by Anand Guru

Last updated 5/2020 English English

₹455 ~~₹1,280~~ 64% off

5 hours left at this price!

30-Day Money-Back Guarantee

What you'll learn

- ✓ Security Analyst/SOC Analyst interview questions and how to answer them
- ✓ Tricky questions and how to answer them
- ✓ Scenario based questions
- ✓ SOC Analyst Training
- ✓ Wide range of topics covered in a SOC Interview
- ✓ How to answer experience related questions
- ✓ Ready-to-use sample CVs for SOC Analyst role

This course includes:

- 2.5 hours on-demand video
- 2 articles
- 8 downloadable resources
- Full lifetime access
- Access on mobile and TV
- Certificate of completion